PRINTING MEDIA AND METHODS EMPLOYING DIGITAL WATERMARKING

Related Application Data

The present application is a continuation-in-part of each of the following applications:

- 09/127,502, filed July 31, 1998 (attached as Appendix A), which is a continuation-in-part of 08/967,693, filed November 12, 1997 (now Patent 6,122,392), which is a continuation of 08/614,521, filed March 15, 1996 (now Patent 5,745,604), which is a continuation of 08/215,289, filed March 17, 1994, now abandoned;
- 09/498,223, filed February 3, 2000 (attached as Appendix B), which is a continuation in part of 09/287,940, filed April 7, 1999, which claims priority to 60/082,228, filed April 16, 1998; the '223 application also claims priority to 09/433,104, filed November, 3, 1999 (attached as Appendix C), which is a continuation in part of 09/234,780, filed January 20, 1999, which is a continuation in part of application 60/071,983 filed January 20, 1998; and
- 09/553,112, filed April 20, 2000 (attached as Appendix D), which claims priority from application 60/131,005, filed April 22, 1999;
- 09/562,516, filed May 1, 2000 (attached as Appendix E)
- 09/562,524, filed May 1, 2000 (attached as Appendix F);
- 09/571,422, filed May 15, 2000 (attached as Appendix G);
- 09/619,264, filed July 19, 2000 (attached as Appendix H);
- 09/629,401, filed August 1, 2000 (attached as Appendix I);
- 09/631,409, filed August 3, 2000 (attached as Appendix J);
- 09/633,587, filed August 7, 2000, which is a continuation-in-part of 09/343,104, filed June 29, 1999, which is a continuation-in-part of 09/314,648, filed May 19, 1999.
- 09/640,806, filed August 17, 2000;

- 09/689,289, filed October 11, 2000 (attached as Appendix K), which is a continuation-in-part of 09/567,405, filed May 8, 2000;
- Application 09/_____, filed March 9, 2001 [attorney docket EWG-140 - Watermarking a Carrier on Which an Image Will be Placed or Projected] (attached as Appendix L).

Claims directed to blank paper media have earlier issued to the present assignee in patents 5,850,481, 5,822,436 and 6,111,954, and have been indicated as allowable (subject to Terminal Disclaimer) in application 09/640,806.

Field of the Invention

The present invention relates to steganographic encoding of substrates - such as blank paper, wherein the encoding is not apparent or conspicuous to human observers, yet is detectable by visible light scanning of the media.

Background and Summary of the Invention

In a great variety of applications, it is desirable for documents and other substrates to convey digital information.

Printed bar codes are one way of encoding digital data on documents, but bar codes are unsuited for many applications due to aesthetics, etc. Magnetic stripes can be used in some circumstances, but again the stripe is conspicuous, and reading the stripe requires a reader device that is not generally available. Radio frequency ID (RFID) is another technology that is sometimes used, but the cost is prohibitive for most applications, and specialized readers are again required.

For those situations in which the marking needs to be both inconspicuous and low cost, digital watermarking offers a promising alternative. Digital watermarking involves making subtle changes to a substrate's appearance (e.g., by ink speckling, texturing, background printing, or other techniques detailed in the literature) – changes that generally pass unnoticed by human viewers but that can be sensed by optical techniques (e.g., webcams, scanners, digital cameras) and decoded by computer processing of the resulting image data to extract the encoded information. Application 09/503,881 details

illustrative watermark encoding/decoding technology. A great number of other techniques are known to artisans in the field, and can be alternatively used. (The following specification commonly uses the term "watermarking" as shorthand for "digital watermarking." This steganographic form of digital data encoding is different than the paper watermarks that have, for centuries, been used in certain documents.)

The present assignee has filed many patent applications that have dealt with digital watermarking of paper and other substrates. The present application serves to compile these various works into a consolidated filing.

Application 09/640,806, with priority back to application 08/215,289, filed March 17, 1994 (through intervening patents 5,822,436 and 6,111,954) teaches that blank photographic paper and photographic film can be pre-processed – before exposure – to encode digital watermark information. When the paper/film is thereafter developed, the encoded information permeates the exposed image. That application also discusses substrate texturing as a way of effecting digital watermarking.

Application 09/127,502 teaches how a watermark pattern can be formed in the background of a printed document, such as by speckling small droplets of ink, or printing a mesh or weave of very thin lines. Ink-jet, intaglio, offset litho, letterpress, xerography, and other printing processes can be used. Such printing can be used to impart a tint to paper while simultaneously encoding auxiliary data (the watermark payload). Watermark encoding by texturing, such as by use of embossing pressure rollers or intaglio plates, is also discussed. Such processes can be performed by the end-user of the paper, or earlier, e.g., by a paper manufacturer. Moreover, they can be applied to the base substrate, or to a laminate layer (which may be clear) that is applied to the base substrate. The background patterning can encode both the auxiliary data payload, and calibration/orientation information that helps the decoder determine (and compensate for) rotation or scaling of the scan data prior to decoding. The encoding can extend across the entire document/substrate, or can be restricted to certain areas.

Application 09/562,524 particularly considers watermarking of laminate layers and synthetic substrates by techniques including opacification, laser ablation and cutting,

and gravure printing. This application also considers how a single sheet of blank media can be encoded to convey different watermarks in different regions.

Application 09/562,516 details a variety of techniques for digitally encoding blank media, including printing watermark patterns with inks whose spectral response extends into UV or IR, and printing with combinations of inks. This application also recognizes that the selection of inks can be tailored to the spectra of expected illumination sources.

Application 09/553,112 details how particular line patterns can be designed to encode desired digital watermark information on documents and substrates. According to one method, a watermark tile is first defined – specifying luminance values in different regions. Lines are then formed between different areas in accordance with the values in the watermark tile.

Applications 09/571,422 and 09/633,587 detail how a printed document, such as a business card, greeting card, product packaging, postal mail, catalog, magazine, credit card, office document, driver's license, book jacket, event ticket, etc., can be encoded with a digital watermark that corresponds to an electronic address. When presented to an imaging system, such as a webcam-equipped computer or other device, the resulting image data is processed to decode the watermark. The device then establishes a link to the electronic address in order to provide the user with additional information or content related to the original document, or to trigger an associated action. (The electronic address can be literally encoded in the watermark. More commonly, however, the watermark encodes an identifier. After detection, the decoding device uses this identifier to access a data structure, such as a remote database, to obtain a corresponding address.) These applications also contemplate that the encoding can be applied to blank media, such as blank magazine paper stock, and blank Post-It brand adhesive note pages. After end use by a consumer, the encoding persists, permitting linking or other watermark-based functionality.

Application 09/631,409 expands on the foregoing – particularly considering systems that link from invoices, bank statements and checks, and other account paperwork to associated on-line resources. By such arrangements, consumers can review

billing history, make electronic payments, correspond with the banking or commercial institution, print completed checks, etc.

Applications 09/498,223 and 09/433,104 detail "fragile" digital watermarks, i.e., watermarks that are designed to be lost, or to degrade in a predictable manner, when subject to certain forms of processing (e.g., scanning and printing, or photocopying). A watermark may be made fragile in numerous ways. One form of fragility relies on low watermark amplitude. That is, the strength of the watermark is only marginally above the minimum needed for detection. If any significant fraction of the signal is lost, as typically occurs in photocopying operations, the watermark becomes unreadable. Another form of fragility relies on the watermark's frequency spectrum. High frequencies are typically attenuated in the various sampling operations associated with digital scanning and printing. Even a high amplitude watermark signal can be significantly impaired, and rendered unreadable, by such photocopying operations. Fragile watermarks can be combined with more traditional, "robust" watermarks within a single document. The former serves to authenticate the document as an original. The latter serves to tag the document with a persistent set of auxiliary data (which can be used for any of the purposes for which watermarks are used).

Application 09/689,289 details particular applications of document watermarking in fields relating to stationary, postal mail and postage. Exemplary applications include document serialization, authentication, copy-control, envelope franking, internet linking, encoding of delivery address information, etc. Again, watermarking of blank printing stock is contemplated. Large lots of documents can be watermarked with the same data payload, or each sheet can convey a unique watermark payload. Corporate stationary can be marked with a fragile watermark to permit a genuine document to be distinguished from a photocopy or other reproduction.

Application 09/619,264 details that printers (including fax machines, photocopiers, etc.) can include optical sensors and decode watermark information from blank paper stock. This watermark can signal to the printer the particular type of paper about to be printed (e.g., glossy photo stock, corporate letterhead, etc.). The printer can then tailor its printing attributes in accordance with the particular paper being printed.

The substrate watermark can be implemented using a variety of techniques, including clear inking.

Application 09/629,401 details how office documents, such as printed spreadsheets, can include a background (or other) watermark pattern. When presented to a webcam, or other such device, an associated computer can decode the watermark and, from this information, identify where the document is stored. The document can then be loaded from such storage, and a corresponding program launched to permit on-screen review or editing. Meta-data associated with the document can also be recalled by reference to the watermark. The encoding of the watermark in the printed output can be effected transparently to the user, such as by the application program (Excel), by printer driver software, or by the printer itself.

Application _____ [attorney docket EWG-140] details how a substrate can be treated so that, when printed with unwatermarked text or imagery, the resulting document will be watermarked. This can be done, e.g., by locally tailoring the ink absorption attributes of different regions on the page, such as by a finely patterned waxy coating.

The foregoing summaries are necessarily abbreviated and incomplete; the reader is referred to the cited applications for their full disclosures. Moreover, the disclosures discussed in connection with one application or technology may have antecedents in earlier applications. Again, the reader is referred to the cited applications.

Certain of the cited applications note that document identification technologies other than digital watermarking (e.g., bar codes, RFIDs, etc.) can be used in certain circumstances.

The above-referenced patents and patent applications are incorporated herein as if set forth in their entireties.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof. (Claims follow appendices.)

APPENDIX A

DIGITAL WATERMARKS AND METHODS FOR SECURITY DOCUMENTS

Related Application Data

This application is a continuation-in-part of the following copending applications, the disclosures of which are incorporated by reference:

? application 09/074,034, filed May 6, 1998;

? application 08/967,693, filed November 12, 1997, which is a continuation of application 08/614,521, filed March 15, 1996 (now Patent 5,745,604), which is a continuation of application 08/215,289, filed March 17, 1994 (now abandoned);

? application 08/649,419, filed May 16, 1996;

? provisional application 60/082,228, filed April 16, 1998 (the specification of which is attached as Appendix A).

The subject matter of this application is also related to that of the present assignee's other issued patents (5,636,292, 5,710,834, 5,721,788, 5,748,763, 5,748,783, 5,768,426), allowed applications (08/438,159, 08/508,083, 08/534,005, 08/637,531, 08/763,847, and 08/969,072) and pending applications (08/746,613 and 08/951,858).

Field of the Invention

The present invention relates to methods and systems for inconspicuously embedding binary data in security documents, and associated methods/systems for detecting/decoding such data. ("Security document" is used herein to refer to negotiable financial instruments (e.g. banknotes, travelers checks, bearer bonds), passports, visas, other immigration documents, stock certificates, postal stamps, lottery tickets, sports/concert tickets, etc.) One application of this the invention is in discouraging counterfeiting of security documents. Another is in transferring machine-readable information through such documents, without alerting human viewers to the presence of such information.

Background and Summary of the Invention

Digital watermarking (sometimes termed "data hiding" or "data embedding") is a growing field of endeavor, with several different approaches. The present assignee's work is reflected in the patents and applications detailed above, together with laid-open PCT application WO97/43736 (attached as Appendix B). Other work is illustrated by U.S. patents 5,734,752, 5,646,997, 5,659,726, 5,664,018, 5,671,277, 5,687,191, 5,687,236, 5,689,587, 5,568,570, 5,572,247, 5,574,962, 5,579,124, 5,581,500, 5,613,004, 5,629,770, 5,461,426, 5,743,631, 5,488,664, 5,530,759,5,539,735, 4,943,973, 5,337,361, 5,404,160, 5,404,377, 5,315,098, 5,319,735, 5,337,362, 4,972,471, 5,161,210, 5,243,423, 5,091,966, 5,113,437, 4,939,515, 5,374,976, 4,855,827, 4,876,617, 4,939,515, 4,963,998, 4,969,041, and published foreign applications WO 98/02864, EP 822,550, WO 97/39410, WO 96/36163, GB 2,196,167, EP 777,197, EP 736,860, EP 705,025, EP 766,468, EP 782,322, WO 95/20291, WO 96/26494, WO 96/36935, WO 96/42151, WO 97/22206, WO 97/26733. Some of the foregoing patents relate to visible watermarking techniques. Other visible watermarking techniques (e.g. data glyphs) are described in U.S. patents 5,706,364, 5,689,620, 5,684,885, 5,680,223, 5,668,636, 5,640,647, 5,594,809.

Much of the work in data embedding is not in the patent literature but rather is published in technical articles. In addition to the patentees of the foregoing patents, some of the other workers in this field (whose watermark-related writings can by found by an author search in the INSPEC or NEXIS databases, among others) include I. Pitas, Eckhard Koch, Jian Zhao, Norishige Morimoto, Laurence Boney, Kineo Matsui, A.Z. Tirkel, Fred Mintzer, B. Macq, Ahmed H. Tewfik, Frederic Jordan, Naohisa Komatsu, Joseph O'Ruanaidh, Neil Johnson, Ingemar Cox, Minerva Yeung, and Lawrence O'Gorman.

The artisan is assumed to be familiar with the foregoing prior art.

In the following disclosure it should be understood that references to watermarking encompass not only the assignee's watermarking technology, but can likewise be practiced with any other watermarking technology, such as those indicated above.

Watermarking can be applied to myriad forms of information. The present disclosure focuses on its applications to security documents. However, it should be recognized that the principles discussed below can also be applied outside this area.

Most of the prior art in image watermarking has focused on pixelated imagery (e.g. bit-mapped images, JPEG/MPEG imagery, VGA/SVGA display devices, etc.). In most watermarking techniques, the luminance or color values of component pixels are slightly changed to effect subliminal encoding of binary data through the image. (This encoding can be done directly in the pixel domain, or after the signal has been processed and represented differently – e.g. as DCT or wavelet coefficients, or as compressed data, etc.)

While pixelated imagery is a relatively recent development, security documents -- commonly employing line art -- go back centuries. One familiar example is U.S. paper currency. On the one dollar banknote, for example, line art is used in several different ways. One is to form intricate webbing patterns

(sometimes termed "guilloche patterns") around the margin of the note (generally comprised of light lines on dark background). Another is to form gray scale imagery, such as the portrait of George Washington (generally comprised of dark lines on a light background).

There are two basic ways to simulate grey-scales in security document line art. One is to change the relative spacings of the lines to effect a lightening or darkening of an image region. Fig. 1A shows such an arrangement; area B looks darker than area A due to the closer spacings of the component lines. The other technique is to change the widths of the component lines -- wider lines resulting in darker areas and narrower lines resulting in lighter areas. Fig. 1B shows such an arrangement. Again, area B looks darker than area A, this time due to the greater widths of the component lines. These techniques are often used together. Ultimately, a given region simply has more or less ink.

In my application 08/438,159 I introduced, and in my application 09/074,034 I elaborated on, techniques for watermarking line art by making slight changes to the widths, or positions, of the component lines. Such techniques are further expanded in the present disclosure.

In several of my cited applications, I discussed various "calibration signals" that can be used to facilitate the decoding of watermark data despite corruption of the encoded image, such as by scaling or rotation. Common counterfeiting techniques -- e.g. color photocopying, or scanning/inkjet printing -- often introduce such corruption, whether deliberately or accidentally. Accordingly, it is important that watermarks embedded in security documents be detectable notwithstanding such effects. Calibration signals particularly suited for use with security documents are detailed in this disclosure.

In accordance with embodiments of the present invention, security documents are encoded to convey machine-readable multi-bit binary information (e.g. digital watermarks), usually in a manner not alerting human viewers that such information is present. The documents can be provided with overt or subliminal calibration patterns. When a document incorporating such a pattern is scanned (e.g. by a photocopier), the pattern facilitates detection of the encoded information notwithstanding possible scaling or rotation of the scan data. The calibration pattern can serve as a carrier for the watermark information, or the watermark can be encoded independently. In one embodiment, the watermark and the calibration pattern are formed on the document by an intaglio process, with or without ink. A photocopier responsive to such markings can take predetermined action if reproduction of a security document is attempted. A passport processing station responsive to such markings can use the decoded binary data to access a database having information concerning the passport holder. Some such apparatuses detect both the watermark data and the presence of a visible structure characteristic of a security document (e.g., the U.S. Federal Reserve Seal).

The foregoing and other features and advantages of the present technology will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Figs. 1A and 1B show prior art techniques for achieving grey-scale effects using line art.

Fig. 2 shows a virtual array of grid points that can be imposed on a security document image according to an embodiment of the present invention.

Fig. 3 shows a virtual array of regions that can be imposed on a security document image according to the Fig. 2 embodiment.

Fig. 4 shows an excerpt of Fig. 3 with a line from a line art image passing therethrough.

Fig. 5 shows changes to the width of the line of Fig. 3 to effect watermark encoding.

Fig. 6 shows changes to the position of the line of Fig. 3 to effect watermark encoding.

Figs. 7A and 7B show aspects of watermark and calibration blocks according to an embodiment of the invention.

Fig. 8 shows an illustrative reference grey-scale calibration tile.

Figs. 9A-9C show steps in the design of a weave calibration pattern according to an embodiment of the invention.

Fig. 10 shows the generation of error data used in designing a weave calibration pattern according to an embodiment of the invention.

Fig. 11 is a block diagram of a passport processing station according to another embodiment of the invention.

Fig. 12 is a block diagram of a photocopier according to another embodiment of the invention.

Detailed Description

By way of introduction, the present specification begins with review of techniques for embedding watermark data in line art, as disclosed in my application 09/074,034.

Referring to Fig. 2, the earlier-described technique employs a grid 10 of imaginary reference points arrayed over a line art image. The spacing between points is 250 microns in the illustrated arrangement, but greater or lesser spacings can of course be used.

Associated with each grid point is a surrounding region 12, shown in Fig. 3. As described below, the luminosity (or reflectance) of each of these regions 12 is slightly changed to effect subliminal encoding of binary data.

Region 12 can take various shapes; the illustrated rounded-rectangular shape is representative only. (The illustrated shape has the advantage of encompassing a fairly large area while introducing fewer visual artifacts than, e.g., square regions.) In other embodiments, squares, rectangles, circles, ellipses, etc., can alternatively be employed.

Fig. 4 is a magnified view of an excerpt of Fig. 3, showing a line 14 passing through the grid of points. The width of the line, of course, depends on the particular image of which it is a part. The illustrated line is about 40 microns in width; greater or lesser widths can naturally be used.

In one encoding technique, shown in Fig. 5, the width of the line is controllably varied so as to change the luminosity of the regions through which it passes. To increase the luminosity (or reflectance), the line is made narrower (i.e. less ink in the region). To decrease the luminosity, the line is made wider (i.e. more ink).

Whether the luminance in a given region should be increased or decreased depends on the particular watermarking algorithm used. Any algorithm can be used, by changing the luminosity of regions 12 as the algorithm would otherwise change the luminance or colors of pixels in a pixelated image. (Some watermarking algorithms effect their changes in a transformed domain, such as DCT, wavelet, or Fourier. However, such changes are ultimately manifested as changes in luminance or color.)

In an exemplary algorithm, the binary data is represented as a sequence of -1s and 1s, instead of 0s and 1s. (The binary data can comprise a single datum, but more typically comprises several. In an illustrative embodiment, the data comprises 128 bits, some of which are error-correcting or -detecting bits.)

Each element of the binary data sequence is then multiplied by a corresponding element of a pseudo-random number sequence, comprised of -1s and 1s, to yield an intermediate data signal. Each element of this intermediate data signal is mapped to a corresponding sub-part of the image, such as a region 12. (Commonly, each element is mapped to several such sub-parts.) The image in (and optionally around) this region is analyzed to determine its relative capability to conceal embedded data, and a corresponding scale factor is produced. Exemplary scale factors may range from 0 to 3. The scale factor for the region is then multiplied by the element of the intermediate data signal mapped to the region in order to yield a "tweak" or "bias" value for the region. In the illustrated case, the resulting tweaks can range from -3 to 3. The luminosity of the region is then adjusted in accordance with the tweak value. A tweak value of -3 may correspond to a -5% change in luminosity; -2 may correspond to -2% change; -1 may correspond to -1% change; 0 may correspond to no change; 1 may correspond to +1% change; 2 may correspond to +2% change, and 3 may correspond to +5% change. (This example follows the basic techniques described in the Real Time Encoder embodiment disclosed in patent 5,710,834.)

In Fig. 5, the watermarking algorithm determined that the luminance of region A should be reduced by a certain percentage, while the luminance of regions C and D should be increased by certain percentages.

In region A, the luminance is reduced by increasing the line width. In region D, the luminance is increased by reducing the line width; similarly in region C (but to a lesser extent).

No line passes through region B, so there is no opportunity to change the region's luminance. This is not fatal to the method, however, since the exemplary watermarking algorithm redundantly encodes each bit of data in sub-parts spaced throughout the line art image.

The changes to line widths in regions A and D of Fig. 5 are exaggerated for purposes of illustration. While the illustrated variance is possible, most implementations will typically modulate the line width 3 - 50% (increase or decrease).

(Many watermarking algorithms routinely operate within a signal margin of about +/- 1% changes in luminosity to effect encoding. That is, the "noise" added by the encoding amounts to just 1% or so of the underlying signal. Lines typically don't occupy the full area of a region, so a 10% change to line width may only effect a 1% change to region luminosity, etc. Security documents are different from photographs in that the artwork generally need not convey photorealism. Thus, security documents can be encoded with higher energy than is used in watermarking photographs, provided the result is still aesthetically satisfactory. To illustrate, localized luminance changes on the order of 10% are possible in security documents, while such a level of watermark energy in photographs would generally be considered unacceptable. In some contexts, localized luminance changes of 20, 30, 50 or even 100% are acceptable.)

In the illustrated technique, the change to line width is a function solely of the watermark tweak (or watermark/calibration pattern tweak, as discussed below) to be applied to a single region. Thus, if a line passes through any part of a region to which a tweak of 2% is to be applied, the line width in that region is changed to effect the 2% luminance difference. In variant techniques, the change in line width is a function of the line's position in the region. In particular, the change in line width is a function of the distance between the region's center grid point and the line's closest approach to that point. If the line passes through the grid point, the full 2% change is effected. At successively greater distances, successively smaller changes are applied. The manner in which the magnitude of the tweak changes as a function of line position within the region can be determined by applying one of various interpolation algorithms, such as the bi-linear, bi-cubic, cubic splines, custom curve, etc.

In other variant techniques, the change in line width in a given region is a weighted function of the tweaks for adjoining or surrounding regions. Thus, the line width in one region may be increased or decreased in accordance with a tweak value corresponding to one or more adjoining regions.

Combinations of the foregoing techniques can also be employed.

In the foregoing techniques, it is sometimes necessary to trade-off the tweak values of adjoining regions. For example, a line may pass along a border between regions, or pass through the point equidistant from four grid points ("equidistant zones"). In such cases, the line may be subject to conflicting tweak values -- one region may want to increase the line width, while another may want to decrease the line width. (Or both may want to increase the line width, but differing amounts.) Similarly in cases where the line does not pass through an equidistant zone, but the change in line width is a function of a neighborhood of regions whose tweaks are of different values. Again, known interpolation functions can be employed to determine the weight to be given the tweak from each region in determining what change is to be made to the line width in any given region.

In the exemplary watermarking algorithm, the average change in luminosity across the security document image is zero, so no generalized lightening or darkening of the image is apparent. The localized changes in luminosity are so minute in magnitude, and localized in position, that they are essentially invisible (e.g. inconspicuous/subliminal) to human viewers.

An alternative technique is shown in Fig. 6, in which line position is changed rather than line width.

In Fig. 6 the original position of the line is shown in dashed form, and the changed position of the line is shown in solid form. To decrease a region's luminosity, the line is moved slightly closer to the center of the grid point; to increase a region's luminosity, the line is moved slightly away. Thus, in region A, the line is moved towards the center grid point, while in region D it is moved away.

It will be noted that the line on the left edge of region A does not return to its nominal (dashed) position as it exits the region. This is because the region to the left of region A also is to have decreased luminosity. Where possible, it is generally preferable not to return a line to its nominal position, but instead to permit shifted lines to remain shifted as they enter adjoining regions. So doing permits a greater net line movement within a region, increasing the embedded signal level.

Again, the line shifts in Fig. 6 are somewhat exaggerated. More typical line shifts are on the order of 3 - 50 microns.

One way to think of the Fig. 6 technique is to employ a magnetism analogy. The grid point in the center of each region can be thought of as a magnet. It either attracts or repels lines. A tweak value of -3, for example, may correspond to a strong-valued attraction force; a tweak value of +2 may correspond to a middle-valued repulsion force, etc. In Fig. 6, the grid point in region A exhibits an attraction force (i.e. a negative tweak value), and the grid point in region D exhibits a repulsion force (e.g. a positive tweak value).

The magnetic analogy is useful because the magnetic effect exerted on a line depends on the distance between the line and the grid point. Thus, a line passing near a grid point is shifted more in position than a line near the periphery of the region.

(Actually, the magnetism analogy can serve as more than a conceptual tool. Instead, magnetic effects can be modeled in a computer program and serve to synthesize a desired placement of the lines relative to the grid points. Arbitrarily customized magnetic fields can be used.)

Each of the variants applicable to Fig. 5 is likewise applicable to Fig. 6.

Combinations of the embodiments of Figs. 5 and 6 can of course be used, resulting in increased watermark energy, better signal-to-noise ratio and, in many cases, less noticeable changes.

In still a further technique, the luminance in each region is changed while leaving the line unchanged. This can be effected by sprinkling tiny dots of ink in the otherwise-vacant parts of the region. In high quality printing, of the type used with security documents, droplets on the order of 3 microns in diameter can be deposited. (Still larger droplets are still beyond the perception threshold for most

viewers.) Speckling a region with such droplets (either in a regular array, or random, or according to a desired profile such as Gaussian), can readily effect a 1% or so change in luminosity. (Usually dark droplets are added to a region, effecting a decrease in luminosity. Increases in luminosity can be effected by speckling with a light colored ink, or by forming light voids in line art otherwise present in a region.) (Actually, production realities often mean that many such microdots will not print, but statistically some will.)

In a variant of the speckling technique, very thin mesh lines can be inserted in the artwork -- again to slightly change the luminance of one or more regions (so-called "background tinting").

The following portion of the specification reviews a calibration, or synchronization pattern used in an illustrative security document to facilitate proper registration of the watermark data for decoding. It may be helpful to being by reviewing further details about the illustrative watermarking method.

Referring to Fig. 7A, an exemplary watermark is divided into "cells" that are 250 microns on a side, each conveying a single bit of information. The cells are grouped into a "block" having 128 cells on a side (i.e. 16,384 cells per block). The blocks are tiled across the region being watermarked (e.g. across the face of a security document).

As noted, the watermark payload consists of 128 bits of data. Each bit is represented by 128 different cells within each block. (The mapping of bits to cells can be pseudo-random, sequential, or otherwise.) The 128 "0"s and "1"s of the watermark data are randomized into substantially equal-probability "1"s and "-1"s by a pseudo-random function to reduce watermark visibility. Where a cell has a value of "1," the luminance of the corresponding area of the image is slightly increased; where a cell has a value of "-1," the luminance of the corresponding area of the image is slightly decreased (or vice versa). In some embodiments, the localized changes to image luminance due to the +1/-1 watermark cell values are scaled in accordance with data-hiding attributes of the local area (e.g. to a range of +/- 4 digital numbers) to increase the robustness of the watermark without compromising its imperceptibility.

It should be noted that a single watermark "cell" commonly encompasses a large number of ink droplets. In high resolution printing, as is commonly used in security documents (e.g. 5000 microdroplets per inch), a single watermark cell may encompass a region of 50 droplets by 50 droplets. In other embodiments, a cell may encompass greater or lesser numbers of droplets.

Decoding a watermark requires precise re-registration of the scanned document image, so the watermark cells are located where expected. To facilitate such registration, a calibration signal can be employed.

An exemplary calibration signal is a geometrical pattern having a known Fourier-Mellin transform. As described in application 08/649,419, when a known pattern is transformed into the Fourier domain, and then further transformed into the Fourier-Mellin domain, the transformed data indicates the scale and rotation of the pattern. If this pattern is replicated on a security document that is thereafter scanned (as noted, scanning commonly introduces rotation, and sometimes scaling), the F-M transform

data indicates the scale and rotation of the scanned data, facilitating virtual re-registration of the security document image for watermark detection.

As shown in Fig. 7B, an illustrative geometrical calibration pattern is a block, 3.2 cm on a side. The block comprises a 16 x 16 array of substantially identical tiles, each 2 mm on a side. Each tile, in term, comprises an 8 x 8 array of component cells.

As described below, the geometrical calibration pattern in the illustrated embodiment is a visible design feature on the security document. Accordingly, unlike the watermark data, the calibration pattern does not have to be limited to a small range of digital numbers in order to keep it substantially hidden among other features of the document. Also unlike the watermark data, the illustrated calibration pattern is not locally scaled in accordance with data hiding attributes of the security document image.

It is possible to print rectangular grids of grey-scaled ink on a document to serve as a calibration pattern. However, aesthetic considerations usually discourage doing so. Preferable is to realize the calibration pattern in a more traditional art form, such as a seemingly random series of intertwining lines, forming a weave-like pattern that is printed across part or all of the document.

To create this weave-like calibration pattern, a designer first defines an 8 x 8 cell reference calibration tile. Each cell in the tile is assigned a grey-scale value. In the illustrated embodiment, values within 2-10 percent of each other are used, although this is not essential. An exemplary reference calibration tile is shown in Fig. 8 (assuming 8-bit quantization).

The Fourier-Mellin transform of a block derived from this reference calibration tile will serve as the key by which the scale and rotation of a scanned security document image are determined.

There is some optimization that may be done in selecting/designing the pattern of grey-scale values that define the reference calibration tile. The pattern should have a F-M transform that is readily distinguished from those of other design and watermark elements on the security document. One design procedure effects a trial F-M transform of the rest of the security document design, and works backwards from this data to select a reference calibration tile that is readily distinguishable.

Once a reference tile pattern is selected, the next steps iteratively define a tile having a weave-like pattern whose local luminance values approximately match the reference tile's grey-scale pattern.

Referring to Fig. 9A, the first such step is to select points on the bottom and left side edges of the tile where lines are to cross the tile boundaries. The angles at which the lines cross these boundaries are also selected. (In the illustrated embodiment, these points and angles are selected arbitrarily, although in other embodiments, the choices can be made in conformance with an optimizing design procedure.)

The selected points and angles are then replicated on the corresponding right and top edges of the tile. By this arrangement, lines exiting the top of one tile seamlessly enter the bottom of the adjoining tile at the same angle. Likewise, lines exiting either side of a tile seamlessly join with lines in the laterally adjoining blocks.

The designer next establishes trial line paths snaking through the tile (Figs. 9B, 9C), linking arbitrarily matched pairs of points on the tile's edges. (These snaking paths are sometimes termed "worms.") Desirably, these paths pass through each of the 64 component cells forming the tile, with the total path length through each cell being within +/- 30% of the average path length through all cells. (This trial routing can be performed with pencil and paper, but more commonly is done on a computer graphics station, with a mouse, light pen, or other input device being manipulated by the designer to establish the routing.) In the illustrated embodiment, the lines have a width of about 30 - 100 microns, and an average spacing between lines of about 100 - 400 microns, although these parameters are not critical.

Turning next to Fig. 10, the trial tile is assembled with like tiles to form a 16 x 16 trial block (3.2 cm on a side), with a repetitive weave pattern formed by replication of the line pattern defined on the 8 x 8 cell trial tile. This trial block is then converted into grey-scale values. The conversion can be done by scanning a printed representation of the trial block, or by computer analysis of the line lengths and positions. The output is a 128 x 128 array of grey-scale values, each value corresponding to the luminance of a 250 micron cell within the trial block.

This grey-scale data is compared with grey-scale data provided by assembling 256 of the reference calibration tiles (each an 8 x 8 array of cells) into a 16 x 16 calibration pattern block. In particular, the grey-scale array resulting from the trial block is subtracted from the grey-scale array resulting from the reference block, generating a 128 x 128 array of error values. This error data is used to tweak the arrangement of lines in the trial block.

In cells of the trial calibration block where the error value is positive, the line is too long. That is, the pattern is too dark in those cells (i.e. it has a low luminance grey-scale value), due to a surplus of line length (i.e. too much ink). By shortening the line length in those cells, their luminance is increased (i.e. the cell is lightened). Shortening can be effected by straightening curved arcs, or by relocating a line's entrance and exit points in a cell so less distance is traversed through the cell.

Conversely, in cells where the error value is negative, the line is too short. By increasing the line length in such cells, their luminance is decreased (i.e. the cell is darkened). Increasing the line length through a cell can be accomplished by increasing the curvature of the line in the cell, or by relocating a line's entrance and exit points along the boundary of the cell, so more distance is traversed through the cell.

A computer program is desirably employed to effect the foregoing changes in line routing to achieve the desired darkening or lightening of each cell.

After line positions in the trial calibration block have been tweaked in this fashion, the trial block is again converted to grey-scale values, and again subtracted from the reference block. Again, an array of error values is produced. The positions of the lines are then further tweaked in accordance with the error values.

The foregoing steps of tweaking line routes in accordance with error signals, converting anew into grey-scale, and computing new error values, is repeated until the luminance of the resulting weave pattern in the trial block is arbitrarily close to the luminance of the reference block. Four of five iterations of this procedure commonly suffice to converge on a final calibration block.

(It will be noted that the initial tile pattern created by the designer is done at the tile level -- 8 x 8 cells. After the initial trial tile is created, subsequent processing proceeds at the block level (128 x 128 cells). A common result of the iterative design procedure is that the component tiles lose their uniformity. That is, the pattern of lines in a tile at a corner of the final calibration block will generally be slightly different than the pattern of lines in a tile near the center of the block.)

After the final calibration block pattern has been established as above, the blocks are tiled repetitively over some or all of the security document, and can serve either as a background design element, or as a more apparent element of the design. By printing this weave pattern in an ink color close to the paper substrate color, the patterning is highly unobtrusive. (If a highly contrasting ink color is used, and if the pattern extends over most or all of the security document, it may be desirable to employ a brighter luminance paper than otherwise, since the weave pattern effectively darkens the substrate.)

As noted in my application 08/649,419, the Fourier-Mellin transform has the property that the same output pattern is produced, regardless of rotation or scaling of the input image. The invariant output pattern is shifted in one dimension proportional to image rotation, and shifted in another dimension proportional to image scaling. When an image whose F-M transform is known, is thereafter rotated and/or scaled, the degree of rotation and scaling can be determined by observing the degree of shift of the transformed F-M pattern in the two dimensions. Once the rotation and scale are known, reciprocal processing of the image can be performed to restore the image to its original orientation and scale.

In the above-described embodiment, the calibration block pattern has a known F-M transform. When a security document incorporating such a pattern is scanned (e.g. by a photocopier, a flatbed scanner, a facsimile machine, etc.), the resulting data can be F-M transformed. The known F-M pattern is then identified in the transformed data, and its two-dimensional shift indicates the scale and rotation corruption of the scanned security document data. With these parameters known, misregistration of the security document – including scale and rotation corruption -- can be backed-off, and the security document data restored to proper alignment and scale. In this re-registered state, the watermark can be detected. (In alternative embodiments, the original scan data is not processed to remove the scale/rotation effects. Instead, subsequent processing proceeds with the data in its corrupted state, and takes into account the specific corruption factor(s) to nonetheless yield accurate decoding, etc.)

The just-described calibration pattern and design procedure, of course, are just exemplary, and are subject to numerous modifications. The dimensions can be varied at will. It is not essential that the cell size of the calibration tiles match that of the watermark. Nor do the cells sizes need to be integrally

related to each other. Nor does the calibration pattern need to be implemented as lines; other ink patterns can alternatively be used to approximate the grey-scale reference pattern

There is no requirement that the lines snake continuously through the tiles. A line can connect to just a single edge point of a tile, resulting in a line that crosses that tile boundary, but no other. Or a line can both begin and end in a single tile, and not connect to any other.

While darker lines on a lighter background are illustrated, lighter lines on a darker background can alternatively be employed.

The iterative design procedure can employ the F-M transform (or other transform). For example, the trial block pattern can be transformed to the F-M domain, and there compared with the F-M transform of the reference block. An F-M domain error signal can thus be obtained, and the routing of the lines can be changed in accordance therewith.

Although the illustrated embodiment tweaked the cell-based grey-scales of the calibration block by changing line curvature and position, other luminance changing techniques can be employed. For example, the width of the weave lines can be locally changed, or small ink dots can be introduced into certain cell areas.

The foregoing (and following) discussions contemplate that the watermark and/or calibration pattern is printed at the same time as (indeed, sometimes as part of) the line art on the security document. In many applications it is desirable to provide the calibration pattern on the security document substrate prior to printing. The markings can be ink applied by the manufacturer, or can be embossings applied, e.g., by rollers in the paper-making process. (Such textural marking is discussed further below.) Or, the markings can be applied by the security document printer, as a preliminary printing operation, such as by offset printing. By using an ink color/density that is already closely matched to the underlying tint of the paper stock, the manufacturer of the paper can introduce less tinting during its manufacture. Such tinting will effectively be replaced by the preliminary printing of the watermark/calibration pattern on the blank paper.

Calibration signals entirely different than those detailed above can also be used. Calibration signals that are optimized to detect rotation, but not scaling, can be employed when scaling is not a serious concern. DCT and Fourier transforms provide data that is readily analyzed to determine rotation. A calibration signal can be tailored to stand out in a typically low-energy portion of the transformed spectrum (e.g. a series of fine lines at an inclined angle transforms to a usually vacant region in DCT space), and the scanned image can be transformed to the DCT/Fourier domains to examine any shift in the calibration signal (e.g. a shift in the spatial frequency representation of the inclined lines).

In some security documents, the just-described calibration weave is printed independently of the watermark encoding. In other embodiments, the weave serves as the lines whose widths, locations, etc., are modulated by the watermark data, as detailed herein and in application 09/074,034.

In an illustrative embodiment, the printing of the security document is achieved by intaglio printing. Intaglio is a well known printing process employing a metal plate into which the security document pattern is etched or engraved. Ink is applied to the plate, filling the etched recesses/grooves. Paper is then pressed into the plate at a very high pressure (e.g. 10 - 20 tons), both raised-inking and slightly deforming (texturing) the paper.

Although ink is commonly used in the intaglio process, it need not be in certain embodiments of the present invention. Instead, the paper texturing provided by the intaglio pressing – alone -- can suffice to convey watermark data. (Texturing of a medium to convey watermark information is disclosed in various of my prior applications, including allowed application 08/438,159.)

To illustrate, an intaglio plate was engraved (using a numerically controlled engraving apparatus), to a depth of slightly less than 1 mm, in accordance with a 3.2 x 3.2 cm. noise-like block of watermark data. The watermark data was generated as described above (e.g. 128 bits of data, randomly distributed in a 128 x 128 cell array), and summed with a correspondingly-sized block of calibration data (implemented as discrete grey-scaled cells, rather than the line/weave pattern detailed above). In this embodiment, the data was not kept within a small range of digital numbers, but instead was railed to a full 8-bit dynamic range.) Banknote paper was intaglio-pressed into this plate -- without ink -- yielding a generally flat substrate with a 3.2 x 3.2 cm textured region therein. Only on fairly close inspection was the texturing visible; on casual inspection the paper surface appeared uniform.

This textured paper was placed – textured extrema down – on the platen of an conventional flatbed scanner (of the sort commonly sold as an accessory for personal computers), and scanned. The resulting image data was input to Adobe's Photoshop image processing software, version 4.0, which includes Digimarc watermark reader software. The software readily detected the watermark from the textured paper, even when the paper was skewed on the scanner platen.

The optical detection process by which a seemingly blank piece of paper can reliably convey 128 bits of data through an inexpensive scanner has not been analyzed in detail; the degree of localized reflection from the paper may be a function of whether the illuminated region is concave or convex in shape. Regardless of the explanation, it is a remarkable phenomenon to witness.

A second experiment was conducted with the same engraved plate, this time using transparent ink. The results were similar, although detection of the watermark data was not always as reliable as in the inkless case. The raised transparent ink may serve as light conduit, dispersing the incident illumination in unpredictable ways as contrasted with simple reflection off un-inked paper.

Experiments have also been conducted using traditional opaque inks. Again, the watermark can reliably be read.

In addition to the just-described technique for "reading" intaglio markings by a conventional scanner, a variant technique is disclosed in Van Renesse, Optical Inspection Techniques for Security

Instrumentation, SPIE Proc. Vol. 2659, pp. 159-167 (1996), and can alternatively be used in embodiments according to the present invention.

Although intaglio is a preferred technique for printing security documents, it is not the only such technique. Other familiar techniques by which watermarks and calibration patterns can be printed include offset litho and letterpress, as well as inkjet printing, xerographic printing, etc. And, as noted, textured watermarking can be effected as part of the paper-making process, e.g. by high pressure textured rollers.

In still other embodiments, the watermark and/or calibration ("information") patterns are not printed on the security document substrate, but rather are formed on or in an auxiliary layer that is laminated with a base substrate. If a generally clear laminate is used, the information patterns can be realized with opaque inks, supplementing the design on the underlying substrate. Or the added information can be encoded in textural form. Combinations of the foregoing can similarly be used.

To retrofit existing security document designs with information patterns, the existing artwork must be modified to effect the necessary additions and/or tweaks to localized security document luminance and/or texture.

When designing new security documents, it would be advantageous to facilitate integration of information patterns into the basic design. One such arrangement is detailed in the following discussion.

Many security documents are still designed largely by hand. A designer works at a drafting table or computer workstation, and spends many hours laying-out minute (e.g. 5 mm x 5 mm) excerpts of the design. To aid integration of watermark and/or calibration pattern data in this process, an accessory layout grid can be provided, identifying the watermark "bias" (e.g. -3 to +3) that is to be included in each 250 micron cell of the security document. If the accessory grid indicates that the luminance should be slightly increased in a cell (e.g. 1%), the designer can take this bias in mind when defining the composition of the cell and include a touch less ink than might otherwise be included. Similarly, if the accessory grid indicates that the luminance should be somewhat strongly increased in a cell (e.g. 5%), the designer can again bear this in mind and try to include more ink than might otherwise be included. Due to the substantial redundancy of most watermark encoding techniques, strict compliance by the designer to these guidelines is not required. Even loose compliance can result in artwork that requires little, if any, further modification to reliably convey watermark and/or calibration information.

Such "designing-in" of embedded information in security documents is facilitated by the number of arbitrary design choices made by security document designers. A few examples from U.S. banknotes include the curls in the presidents' hair, the drape of clothing, the clouds in the skies, the shrubbery in the landscaping, the bricks in the pyramid, the fill patterns in the lettering, and the great number of arbitrary guilloche patterns and other fanciful designs, etc. All include curves, folds, wrinkles, shadow effects, etc., about which the designer has wide discretion in selecting local luminance, etc. Instead of making such choices arbitrarily, the designer can make these choices deliberately so as to serve an informational -- as well as an aesthetic -- function.

To further aid the security document designer, data defining several different information-carrying patterns (both watermark and/or calibration pattern) can be stored on mass storage of a computer a workstation and serve as a library of design elements for future designs. The same user-interface techniques that are employed to pick colors in image-editing software (e.g. Adobe Photoshop) and fill textures in presentation programs (e.g. Microsoft PowerPoint) can similarly be used to present a palette of information patterns to a security document designer. Clicking on a visual representation of the desired pattern makes the pattern available for inclusion in a security document being designed (e.g. filling a desired area).

In the embodiment earlier-described, the calibration pattern is printed as a visible artistic element of the security document. However, the same calibration effect can be provided subliminally if desired. That is, instead of generating artwork mimicking the grey-scale pattern of the reference calibration block, the reference calibration block can itself be encoded into the security document as small changes in local luminance. In many such embodiments, the bias to localized document luminance due to the calibration pattern is simply added to the bias due to the watermark data, and encoded like the watermark data (e.g. as localized changes to the width or position of component line-art lines, as inserted ink droplets, etc.).

The uses to which the 128 bits of watermark data can be put in security documents are myriad. Many are detailed in the materials cited above. Examples include postal stamps encoded with their value, or with the zip code of the destination to which they are addressed (or from which they were sent); banknotes encoded with their denomination, and their date and place of issuance; identification documents encoded with authentication information by which a person's identify can be verified; etc., etc.

The encoded data can be in a raw form – available to any reader having the requisite key data (in watermarking techniques where a key data is used), or can be encrypted, such as with public key encryption techniques, etc. The encoded data can embody information directly, or can be a pointer or an index to a further collection of data in which the ultimate information desired is stored.

For example, watermark data in a passport need not encode a complete dossier of information on the passport owner. Instead, the encoded data can include key data (e.g. a social security number) identifying a particular record in a remote database in which biographical data pertaining to the passport owner is stored. A passport processing station employing such an arrangement is shown in Fig. 11.

To decode watermark data, the security document must be converted into electronic image data for analysis. This conversion is typically performed by a scanner.

Scanners are well known, so a detailed description is not provided here. Suffice it to say that scanners conventionally employ a line of closely spaced photodetector cells that produce signals related to the amount of the light reflected from successive swaths of the document. Most inexpensive consumer scanners have a resolution of 300 dots per inch (dpi), or a center to center spacing of component photodetectors of about 84 microns. Higher quality scanners of the sort found in most professional imaging equipment and photocopiers have resolutions of 600 dpi (42 microns), 1200 dpi (21 microns), or better.

Taking the example of a 300 dpi scanner (84 micron photodetector spacing), each 250 micron region 12 on the security document will correspond to about a 3 x 3 array of photodetector samples. Naturally, only in rare instances will a given region be physically registered with the scanner so that nine photodetector samples capture the luminance in that region, and nothing else. More commonly, the image is rotated with respect to the scanner photodetectors, or is longitudinally misaligned (i.e. some photodetectors image sub-parts of two adjoining regions). However, since the scanner oversamples the regions, the luminance of each region can unambiguously be determined.

In one embodiment, the scanned data from the document is collected in a two dimensional array of data and processed to detect the embedded calibration information. The scanner data is then processed to effect a virtual re-registration of the document image. A software program next analyzes the statistics of the re-registered data (using the techniques disclosed in my prior writings) to extract the bits of the embedded data.

(Again, the reference to my earlier watermark decoding techniques is exemplary only. Once scanning begins and the data is available in sampled form, it is straightforward to apply any other watermark decoding technique to extract a correspondingly-encoded watermark. Some of these other techniques employ domain transformations (e.g. to wavelet, DCT, or Fourier domains, as part of the decoding process).)

In a variant embodiment, the scanned data is not assembled in a complete array prior to processing. Instead, it is processed in real-time, as it is generated, in order to detect embedded watermark data without delay. (Depending on the parameters of the scanner, it may be necessary to scan a half-inch or so of the document before the statistics of the resulting data unambiguously indicate the presence of a watermark.)

In other embodiments, hardware devices are provided with the capability to recognize embedded watermark data in any document images they process, and to respond accordingly.

One example is a color photocopier. Such devices employ a color scanner to generate sampled (pixel) data corresponding to an input media (e.g. a dollar bill). If watermark data associated with a security document is detected, the photocopier can take one or more steps.

One option is simply to interrupt copying, and display a message reminding the operator that it is illegal to reproduce currency.

Another option is to dial a remote service and report the attempted banknote reproduction. Photocopiers with dial-out capabilities are known in the art (e.g. patent 5,305,199) and are readily adapted to this purpose. The remote service can be an independent service, or can be a government agency.

Yet another option is to permit the copying, but to insert forensic tracer data in the resultant copy. This tracer data can take various forms. Steganographically encoded binary data is one example. An example is shown in patent 5,568,268. The tracer data can memorialize the serial number of the machine

that made the copy and/or the date and time the copy was made. To address privacy concerns, such tracer data is not normally inserted in all photocopied output, but is inserted only when the subject being photocopied is detected as being a security document. (An example of such an arrangement is shown in Fig. 12.)

Desirably, the scan data is analyzed on a line-by-line basis in order to identify illicit photocopying with a minimum of delay. If a security document is scanned, one or more lines of scanner output data may be provided to the photocopier's reprographic unit before the recognition decision has been made. In this case the photocopy will have two regions: a first region that is not tracer-marked, and a second, subsequent region in which the tracer data has been inserted.

Photocopiers with other means to detect not-to-be-copied documents are known in the art, and employ various response strategies. Examples are detailed in U.S. Patents 5,583,614, 4,723,149, 5,633,952, 5,640,467, and 5,424,807.

Another hardware device that can employ the foregoing principles is a standalone scanner. A programmed processor (or dedicated hardware) inside the scanner analyzes the data being generated by the device, and responds accordingly.

Yet another hardware device that can employ the foregoing principles is a printer. A processor inside the device analyzes graphical image data to be printed, looking for watermarks associated with security documents.

For both the scanner and printer devices, response strategies can include disabling operation, or inserting tracer information. (Such devices typically do not have dial-out capabilities.)

Again, it is desirable to process the scanner or printer data as it becomes available, so as to detect any security document processing with a minimum of delay. Again, there will be some lag time before a detection decision is made. Accordingly, the scanner or printer output will be comprised of two parts, one without the tracer data, and another with the tracer data.

Many security documents already include visible structures that can be used as aids in banknote detection (e.g. the Federal Reserve seal, and various geometrical markings on U.S. currency). In accordance with a further aspect of the present invention, a security document is analyzed by an integrated system that considers both the visible structures and watermark-embedded data.

Visible security document structures can be sensed using known pattern recognition techniques. Examples of such techniques are disclosed in U.S. Patents 5,321,773, 5,390,259, 5,533,144, 5,539,841, 5,583,614, 5,633,952, 4,723,149, 5,692,073, and 5,424,807 and laid-open foreign applications EP 649,114 and EP 766,449.

In photocopiers (and the like) equipped to detect both visible structures and watermarks from security documents, the detection of <u>either</u> can cause one or more of the above-noted responses to be initiated (Fig. 12).

Again, scanners and printers can be equipped with a similar capability – analyzing the data for either of these security document hallmarks. If either is detected, the software (or hardware) responds accordingly.

Identification of security documents by watermark data provides an important advantage over recognition by visible structures -- it cannot so easily be defeated. A security document can be doctored (e.g. by white-out, scissors, or less crude techniques) to remove/obliterate the visible structures. Such a document can then be freely copied on either a visible structure-sensing photocopier or scanner/printer installation. The removed visible structure can then be added back in via a second printing/photocopying operation. If the printer is not equipped with security document-disabling capabilities, image-editing tools can be used to insert visible structures back into image data sets scanned from such doctored documents, and the complete document can then be freely printed. By additionally including embedded watermark data in the security document, and sensing same, such ruses will not succeed.

(A similar ruse is to scan a security document image on a non-security document-sensing scanner. The resulting image set can then be edited by conventional image editing tools to remove/obliterate the visible structures. Such a data set can then be printed – even on a printer/photocopier that examines such data for the presence of visible structures. Again, the missing visible structures can be inserted by a subsequent printing/photocopying operation.)

Desirably, the visible structure detector and the watermark detector are integrated together as a single hardware and/or software tool. This arrangement provides various economies, e.g., in interfacing with the scanner, manipulating pixel data sets for pattern recognition and watermark extraction, electronically re-registering the image to facilitate pattern recognition/watermark extraction, issuing control signals (e.g. disabling) signals to the photocopier/scanner, etc.

While the foregoing apparatuses are particularly concerned with counterfeit deterrence, the embedded markings can also serve other functions. Examples include banknote processing machines that perform denomination sorting, counterfeit detection, and circulation analysis functions. (I.e., banknotes with certain markings may be distributed through known sources, and their circulation/distribution can subsequently be monitored to assist in macro-economic analyses.)

From the foregoing, it will be recognized that various embodiments according to the present invention provide techniques for embedding multi-bit binary data in security documents, and provide for the reliable extraction of such data even in the presence of various forms of corruption (e.g. scale and rotation).

(To provide a comprehensive disclosure without unduly lengthening the following specification, applicants incorporate by reference the patents and applications cited above.)

Having described and illustrated the principles of my invention with reference to several illustrative embodiments, it will be recognized that these embodiments are exemplary only and should not be taken as limiting the scope of my invention. Guided by the foregoing teachings, it should be apparent

that other watermarking, decoding, and anti-counterfeiting technologies can be substituted for, and/or combined with, the elements detailed above to yield advantageous effects. Other features disclosed in my earlier applications can similarly be employed in embodiments of the technology detailed herein. (Thus, I have not here belabored application of each of the techniques disclosed in my earlier applications -- e.g. use of neural networks for watermark detectors -- to the present subject matter since same is fairly taught by reading the present disclosure in the context of my earlier work.)

While the technology has been described with reference to embodiments employing regular rectangular arrays of cells, those skilled in the art will recognize that other arrays -- neither rectangular nor regular -- can alternatively be used.

While the embodiments have described the calibration patterns as adjuncts to digital watermarks -- facilitating their detection, such patterns have utility apart from digital watermarks. One example is in re-registering scanned security document image data to facilitate detection of visible structures (e.g. detection of the Federal Reserve seal, using known pattern recognition techniques). Indeed, the use of such calibration patterns to register both watermark and visible structure image data for recognition is an important economy that can be gained by integration a visible structure detector and a watermark detector into a single system.

Although security documents have most commonly been printed (e.g. cotton/linen), other substrates are gaining in popularity (e.g. synthetics, such as polymers) and are well (or better) suited for use with the above-described techniques.

The embodiments detailed above can be implemented in dedicated hardware (e.g. ASICs), programmable hardware, and/or software.

In view of the many possible embodiments to which the principles of the above-described technology may be put, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of my invention. Rather, I claim as my invention all such embodiments as may come within the scope and spirit of the following claims and equivalents thereto.

I CLAIM:

1. A security document including at least a substrate, a digital watermark, and a calibration pattern, the calibration pattern having a known transform facilitating decoding of the digital watermark from scan data corresponding to said document.

2. The document of claim 1 in which the calibration pattern has a known Fourier-Mellin transform facilitating decoding of the digital watermark from scan data corresponding to said document.

3. A negotiable financial instrument in accordance with claim 1.

4. A passport in accordance with claim 1.

5. The document of claim 1 in which the calibration pattern has a visible weave-like appearance.

6. The document of claim 1 in which the calibration pattern extends across most of the security document.

7. The document of claim 1 in which at least one of the digital watermark and calibration pattern are realized by texturing of the document, and not printing.

8. The document of claim 1 in which both the digital watermark and the calibration pattern are realized by texturing of the document, and not printing.

9. The document of claim 1 in which each one square millimeter zone of the calibration pattern has an 8-bit grey-scale value within twenty percent of the value of all adjoining one square millimeter zones of the calibration pattern.

10. The document of claim 1 in which each 250 micron by 250 micron zone of the calibration pattern has an 8-bit grey-scale value within twenty percent of the value of all adjoining 250 micron by 250 micron zones of the calibration pattern.

11. The document of claim 1 in which the calibration pattern comprises a tiled pattern, each tile including a line following an apparently random route.

12. A method of producing a security document, comprising:

providing multi-bit binary data;

forming a pattern of recesses in a metal member, said pattern having the multi-bit binary data encoded therein; and

pressing a substrate into said metal member to texture the substrate in accordance with said binary data.

13. The method of claim 12 further including inking the recesses prior to the pressing.

14. The method of claim 12 in which the pattern has the multi-bit binary data steganographically encoded therein, wherein a human viewer of the texture on the substrate is not alerted that it conveys multi-bit binary data.

15. A method of processing a security document, comprising:

generating scan data corresponding to said document;

performing a domain transformation on the scan data to obtain corruption data related thereto; and

detecting embedded information from the processed scan data, said detecting employing said corruption data.

16. The method of claim 15 in which:

the domain transformation is a Fourier-Mellin transform;

the corruption data is a scale or rotation factor; and

the detecting includes compensating the scan data in accordance with the corruption data.

17. The method of claim 15 in which the embedded information comprises multi-bit digital data.

18. The method of claim 15 which further includes using the detected information to access additional information in a database.

19. Apparatus for use with security documents, comprising:

a scanner for scanning a security document and producing scan data corresponding thereto;

a processor responsive to encoding on the security document for determining rotation of the scan data from a reference state and producing output data corresponding thereto;

a visible structure detector; and

a steganographic watermark detector;

said output data permitting the detectors to detect visible structures and steganographic watermarks associated with the security document notwithstanding at least certain rotations of the scan data.

DIGITAL WATERMARKS AND METHODS FOR SECURITY DOCUMENTS

Abstract of the Disclosure

Security documents (e.g. passports, currency, event tickets, and the like) are encoded to convey machine-readable multi-bit binary information (e.g. digital watermark), usually in a manner not alerting human viewers that such information is present. The documents can be provided with overt or subliminal calibration patterns. When a document incorporating such a pattern is scanned (e.g. by a photocopier), the pattern facilitates detection of the encoded information notwithstanding possible scaling or rotation of the scan data. The calibration pattern can serve as a carrier for the watermark information, or the watermark can be encoded independently. In one embodiment, the watermark and the calibration pattern are formed on the document by an intaglio process, with or without ink. A photocopier responsive to such markings can take predetermined action if reproduction of a security document is attempted. A passport processing station responsive to such markings can use the decoded binary data to access a database having information concerning the passport holder. Some such apparatuses detect both the watermark data and the presence of a visible structure characteristic of a security document (e.g., the U.S. Federal Reserve Seal).

APPENDIX B

DIGITAL WATERMARKING EMPLOYING BOTH FRAIL AND ROBUST WATERMARKS

Related Application Data

This application is a continuation-in-part of copending application 09/287,940, filed April 7, 1999, which claims priority to abandoned application 60/082,228, filed April 16, 1998. This application is also a continuation of copending application 09/433,104, filed November 3, 1999, which is a continuation-in-part of copending application 09/234,780, filed January 20, 1999, which claims priority to abandoned application 60/071,983, filed January 20, 1998.

Field of the Invention

The present application relates to digital watermarking, and particularly relates to digital watermarking techniques employing both frail and robust watermarks.

Background and Summary of the Invention

For expository convenience, the following discussion focuses on an exemplary application of the disclosed technology – encoding the images printed on banknotes with both frail and robust watermarks. As noted later, however, the technology also finds application beyond image watermarking, including in video and audio watermarking.

The problem of casual counterfeiting of banknotes first arose two decades ago, with the introduction of color photocopiers. A number of techniques were proposed to address the problem.

U.S. Patent 5,659,628 (assigned to Ricoh) is one of several patents noting that photocopiers can be equipped to recognize banknotes and prevent their photocopying. The Ricoh patent particularly proposed that the red seal printed on Japanese yen notes is a pattern well-suited for machine recognition. U.S. Patents 5,845,008 (assigned to Omron), and 5,724,154 and 5,731,880 (both assigned to Canon) show other photocopiers that sense the presence of the seal emblem on banknotes, and disable a photocopier in response.

Other technologies proposed that counterfeiting might be deterred by uniquely marking the printed output from each color photocopier, so that copies could be traced back to the originating machine. U.S. Patent 5,568,268, for example, discloses the addition of essentially-imperceptible patterns of yellow dots to printed output; the pattern is unique to the machine. U.S. Patent 5,557,742 discloses a related arrangement in which the photocopier's serial number is printed on output documents, again in essentially-imperceptible form (small yellow lettering). U.S. Patent 5,661,574 shows an arrangement in which bits comprising the photocopier's serial number are represented in the photocopier's printed output by incrementing, or decrementing, pixel values (e.g. yellow pixels) at known locations by fixed amounts (e.g. +/-30), depending on whether the corresponding serial number bit is a "1" or a "0."

Recent advances in color printing technology have greatly increased the level of casual counterfeiting. High quality scanners are now readily available to many computer users, with 300 dpi scanners available for under $100, and 600 dpi scanners available for marginally more. Similarly, photographic quality color ink-jet printers are commonly available from Hewlett-Packard Co., Epson, etc. for under $300.

These tools pose new threats. For example, a banknote can be doctored (e.g. by white-out, scissors, or less crude techniques) to remove/obliterate the visible patterns on which prior art banknote detection techniques relied to prevent counterfeiting. Such a doctored document can then be freely scanned or copied, even on photocopiers designed to prevent processing of banknote images. The removed pattern(s) can then be added back in, e.g. by use of digital image editing tools, permitting free reproduction of the banknote.

In accordance with aspects of the present invention, these and other current threats are addressed by digitally watermarking banknotes, and equipping devices to sense such watermarks and respond accordingly.

(Watermarking is a quickly growing field of endeavor, with several different approaches. The present assignee's work is reflected in the earlier-cited related applications, as well as in U.S. Patents 5,841,978, 5,748,783, 5,710,834, 5,636,292, 5,721,788, and laid-open PCT application WO97/43736. Other work is illustrated by U.S. Patents 5,734,752, 5,646,997, 5,659,726, 5,664,018, 5,671,277, 5,687,191, 5,687,236, 5,689,587, 5,568,570, 5,572,247, 5,574,962, 5,579,124, 5,581,500, 5,613,004, 5,629,770, 5,461,426, 5,743,631, 5,488,664, 5,530,759,5,539,735, 4,943,973, 5,337,361, 5,404,160, 5,404,377, 5,315,098, 5,319,735, 5,337,362, 4,972,471, 5,161,210, 5,243,423, 5,091,966, 5,113,437, 4,939,515, 5,374,976, 4,855,827, 4,876,617, 4,939,515, 4,963,998, 4,969,041, and published foreign applications WO 98/02864, EP 822,550, WO 97/39410, WO 96/36163, GB 2,196,167, EP 777,197, EP 736,860, EP 705,025, EP 766,468, EP 782,322, WO 95/20291, WO 96/26494, WO 96/36935, WO 96/42151, WO 97/22206, WO 97/26733. Some of the foregoing patents relate to visible watermarking techniques. Other visible watermarking techniques (e.g. data glyphs) are described in U.S. Patents 5,706,364, 5,689,620, 5,684,885, 5,680,223, 5,668,636, 5,640,647, 5,594,809.

Most of the work in watermarking, however, is not in the patent literature but rather in published research. In addition to the patentees of the foregoing patents, some of the other workers in this field (whose watermark-related writings can by found by an author search in the INSPEC database) include I. Pitas, Eckhard Koch, Jian Zhao, Norishige Morimoto, Laurence Boney, Kineo Matsui, A.Z. Tirkel, Fred Mintzer, B. Macq, Ahmed H. Tewfik, Frederic Jordan, Naohisa Komatsu, and Lawrence O'Gorman.

The artisan is assumed to be familiar with the foregoing prior art.

In the present disclosure it should be understood that references to watermarking encompass not only the assignee's watermarking technology, but can likewise be practiced with any other watermarking technology, such as those indicated above.

The physical manifestation of watermarked information most commonly takes the form of altered signal values, such as slightly changed pixel values, picture luminance, picture colors, DCT coefficients, instantaneous audio amplitudes, etc. However, a watermark can also be manifested in other ways, such as changes in the surface microtopology of a medium, localized chemical changes (e.g. in photographic emulsions), localized variations in optical density, localized changes in luminescence, etc. Watermarks can also be optically implemented in holograms and conventional paper watermarks.)

In accordance with an exemplary embodiment of the present invention, an object - such as a banknote image - is encoded with two watermarks. One is relatively robust, and withstands various types of corruption, and is detectable in the object even after multiple generations of intervening distortion. The other is relatively frail, so that it fails with the first distortion. If a version of the object is encountered having the robust watermark but not the frail watermark, the object can be inferred to have been processed, and thus not an original.

The foregoing and other features and advantages of the present invention will be more readily apparent from the following Detailed Description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 shows part of an automatic teller machine employing principles of the present invention.

Fig. 2 shows part of a device (e.g. a photocopier, scanner, or printer) employing principles of the present invention.

Fig. 3 shows part of another device employing principles of the present invention.

Detailed Description

Watermarks in banknotes and other security documents (passports, stock certificates, checks, etc. – all collectively referred to as banknotes herein) offer great promise to reduce such counterfeiting, as discussed more fully below. Additionally, watermarks provide a high-confidence technique for banknote authentication.

By way of example, consider an automatic teller machine that uses watermark data to provide high confidence authentication of banknotes, permitting it to accept -- as well as dispense -- cash. Referring to Fig. 1, such a machine (11) is provided with a known optical scanner (13) to produce digital data (15) corresponding to the face(s) of the bill (16). This image set (14) is then analyzed (16) to extract embedded watermark data. In watermarking technologies that require knowledge of a code signal (20) for decoding (e.g. noise modulation signal, crypto key, spreading signal, etc.), a bill may be watermarked in accordance with several such codes. Some of these codes are public – permitting their reading by conventional machines. Others are private, and are reserved for use by government agencies and the like. (C.f. public and private codes in the present assignee's issued patents.)

As noted, banknotes presently include certain visible structures, or markings (e.g., the seal emblem noted in the earlier-cited patents), which can be used as aids to note authentication (either by visual inspection or by machine detection). Desirably, a note is examined by an integrated detection system (24), for both such visible structures (22), as well as the present watermark-embedded data, to determine authenticity.

The visible structures can be sensed using known pattern recognition techniques. Examples of such techniques are disclosed in U.S. Patents 5,321,773, 5,390,259, 5,533,144, 5,539,841, 5,583,614, 5,633,952, 4,723,149 and 5,424,807 and laid-open foreign application EP 766,449. The embedded watermark data can be recovered using the scanning/analysis techniques disclosed in the cited patents and publications.

To reduce counterfeiting, it is desirable that document-reproducing technologies recognize banknotes and refuse to reproduce same. Referring to Fig. 2, a photocopier (30), for example, can sense the presence of either a visible structure (32) or embedded banknote watermark data (34), and disable copying if either is present (36). Scanners and printers can be equipped with a similar capability – analyzing the data scanned or to be printed for either of these banknote hallmarks. If either is detected, the software (or hardware) disables further operation.

The watermark detection criteria provides an important advantage not otherwise available. As noted, an original bill can be doctored (e.g. by white-out, scissors, or less crude techniques) to remove/obliterate the visible structures. Such a document can then be freely copied on either a visible structure-sensing photocopier or scanner/printer installation. The removed visible structure can then be added in via a second printing/photocopying operation. If the printer is not equipped with banknote-disabling capabilities, image-editing tools can be used to insert visible structures back into image data sets scanned from such doctored bills, and the complete bill freely printed. By additionally including embedded watermark data in the banknote, and sensing same, such ruses will not succeed.

(A similar ruse is to scan a banknote image on a non-banknote-sensing scanner. The resulting image set can then be edited by conventional image editing tools to remove/obliterate the visible structures. Such a data set can then be printed – even on a printer/photocopier that examines such data for the presence of visible structures. Again, the missing visible structures can be inserted by a subsequent printing/photocopying operation.)

Desirably, the visible structure detector and the watermark detector are integrated together as a single hardware and/or software tool. This arrangement provides various economies, e.g., in interfacing with the scanner, manipulating pixel data sets for pattern recognition and watermark extraction, electronically re-registering the image to facilitate pattern recognition/watermark extraction, issuing control signals (e.g. disabling) signals to the photocopier/scanner, etc.

A related principle (Fig. 3) is to insert an imperceptible watermark having a universal ID (UID) into all documents printed with a printer, scanned with a scanner, or reproduced by a photocopier. The

UID is associated with the particular printer/photocopier/scanner in a registry database maintained by the products' manufacturers. The manufacturer can also enter in this database the name of the distributor to whom the product was initially shipped. Still further, the owner's name and address can be added to the database when the machine is registered for warranty service. While not preventing use of such machines in counterfeiting, the embedded UID facilitates identifying the machine that generated a counterfeit banknote. (This is an application in which a private watermark might best be used.)

While the foregoing applications disabled potential counterfeiting operations upon the detection of either a visible structure or watermarked data, in other applications, both criteria must be met before a banknote is recognized as genuine. Such applications typically involve the receipt or acceptance of banknotes, e.g. by ATMs as discussed above and illustrated in Fig. 1.

The foregoing principles (employing just watermark data, or in conjunction with visible indicia) can likewise be used to prevent counterfeiting of tags and labels (e.g. the fake labels and tags commonly used in pirating Levis brand jeans, branded software, etc.)

The reader may first assume that banknote watermarking is effected by slight alterations to the ink color/density/distribution, etc. on the paper. This is one approach. Another is to watermark the underlying medium (whether paper, polymer, etc.) with a watermark. This can be done by changing the microtopology of the medium (a la mini-Braille) to manifest the watermark data. Another option is to employ a laminate on or within the banknote, where the laminate has the watermarking manifested thereon/therein. The laminate can be textured (as above), or its optical transmissivity can vary in accordance with a noise-like pattern that is the watermark, or a chemical property can similarly vary.

*Another option is to print at least part of a watermark using photoluminescent ink. This allows, e.g., a merchant presented with a banknote, to quickly verify the presence of *some* watermark-like indicia in/on the bill even without resort to a scanner and computer analysis (e.g. by examining under a black light). Such photoluminescent ink can also print human-readable indicia on the bill, such as the denomination of a banknote. (Since ink-jet printers and other common mass-printing technologies employ cyan/magenta/yellow/black to form colors, they can produce only a limited spectrum of colors. Photoluminescent colors are outside their capabilities. Fluorescent colors – such as the yellow, pink and green dyes used in highlighting markers – can similarly be used and have the advantage of being visible without a black light.)*

An improvement to existing encoding techniques is to add an iterative assessment of the robustness of the mark, with a corresponding adjustment in a re-watermarking operation. Especially when encoding multiple bit watermarks, the characteristics of the underlying content may result in some bits being more robustly (e.g. strongly) encoded than others. In an illustrative technique employing this improvement, a watermark is first embedded in an object. Next, a trial decoding operation is performed. A confidence measure (e.g. signal-to-noise ratio) associated with each bit detected in the decoding operation is then assessed. The bits that appear weakly encoded are identified, and corresponding changes are made

to the watermarking parameters to bring up the relative strengths of these bits. The object is then watermarked anew, with the changed parameters. This process can be repeated, as needed, until all of the bits comprising the encoded data are approximately equally detectable from the encoded object, or meet some predetermined signal-to-noise ratio threshold.

The foregoing applications, and others, can generally benefit by multiple watermarks. For example, an object (physical or data) can be marked once in the spatial domain, and a second time in the spatial frequency domain. (It should be understood that any change in one domain has repercussions in the other. Here we reference the domain in which the change is directly effected.)

Another option is to mark an object with watermarks of two different levels of robustness, or strength. The more robust watermark withstands various types of corruption, and is detectable in the object even after multiple generations of intervening distortion. The less robust watermark can be made frail enough to fail with the first distortion of the object. In a banknote, for example, the less robust watermark serves as an authentication mark. Any scanning and reprinting operation will cause it to become unreadable. Both the robust and the frail watermarks should be present in an authentic banknote; only the former watermark will be present in a counterfeit.

Still another form of multiple-watermarking is with content that is compressed. The content can be watermarked once (or more) in an uncompressed state. Then, after compression, a further watermark (or watermarks) can be applied.

Still another advantage from multiple watermarks is protection against sleuthing. If one of the watermarks is found and cracked, the other watermark(s) will still be present and serve to identify the object.

The foregoing discussion has addressed various technological fixes to many different problems. Exemplary solutions have been detailed above. Others will be apparent to the artisan by applying common knowledge to extrapolate from the solutions provided above.

For example, the technology and solutions disclosed herein have made use of elements and techniques known from the cited references. Other elements and techniques from the cited references can similarly be combined to yield further implementations within the scope of the present invention. Thus, for example, holograms with watermark data can be employed in banknotes, single-bit watermarking can commonly be substituted for multi-bit watermarking, technology described as using imperceptible watermarks can alternatively be practiced using visible watermarks (glyphs, etc.), techniques described as applied to images can likewise be applied to video and audio, local scaling of watermark energy can be provided to enhance watermark signal-to-noise ratio without increasing human perceptibility, various filtering operations can be employed to serve the functions explained in the prior art, watermarks can include subliminal graticules to aid in image re-registration, encoding may proceed at the granularity of a single pixel (or DCT coefficient), or may similarly treat adjoining groups of pixels (or DCT coefficients), the encoding can be optimized to withstand expected forms of content corruption. Etc., etc., etc. Thus, the

exemplary embodiments are only selected samples of the solutions available by combining the teachings referenced above. The other solutions necessarily are not exhaustively described herein, but are fairly within the understanding of an artisan given the foregoing disclosure and familiarity with the cited art.

(To provide a comprehensive disclosure without unduly lengthening the following specification, applicants incorporate by reference the patent documents cited herein. Document 09/433,104, for example, contains additional details re multiple watermark technology, such as arrangements employing frail and robust watermarks.)

I CLAIM:

1. A watermarking method characterised by watermarking an object with first and second watermarks, wherein the second watermark is relatively less robust than the first.

2. The method of claim 1 in which the first watermark is designed to withstand a predetermined process, and the second watermark is not.

3. The method of claim 2 in which the predetermined process includes scanning.

4. The method of claim 2 in which the predetermined process includes printing.

5. The method of claim 2 in which the predetermined process includes distortion.

6. The method of claim 1 in which the object comprises an image.

7. The method of claim 6 in which the object comprises a document printed with said image.

8. The method of claim 1 in which the object comprises audio.

9. The method of claim 1 in which the object comprises video.

10. The method of claim 1 that further includes analyzing a suspect object for the presence of the second watermark, the absence of said second watermark indicating that the suspect object is not an original object.

11. The method of claim 1 in which the object includes plural data samples, each sample having a value, and the watermarking changes the values of at least certain of said samples.

12. The method of claim 11 in which said samples comprises pixels.

13. A method comprising:

attempting to detect first and second watermarks from an object;

if the first and second watermarks are both detected, reaching a first conclusion concerning the object; and

if the first watermark is detected but not the second, reaching a second, different, conclusion concerning the object.

DIGITAL WATERMARKING EMPLOYING
BOTH FRAIL AND ROBUST WATERMARKS

Abstract of the Disclosure

Image, video, or audio data is encoded with both a frail and a robust watermark. The two watermarks respond differently to different forms of processing (e.g., copying the object may render the frail watermark unreadable), permitting an original object to be distinguished from a processed object. Appropriate action can then taken in response thereto.

APPENDIX C

METHODS AND SYSTEMS USING MULTIPLE WATERMARKS

Related Applications

The present application is a continuation in part of copending application serial number 09/234,780———, filed January 20, 1999, which is a continuation in part of application 60/071,983 filed January 20, 1998.

Field of the Invention

The present invention relates to steganography, and more particularly relates to the use of multiple watermarks to determine the authenticity or history of a particular document or image.

Background of the Invention

Steganographic and digital watermarking technologies are well known. For example see U.S. Patent 5,636,292 and the extensive references cited therein. Also see copending patent applications serial number 08/327,426 which was filed 10/21/94 and copending application serial number 08/436,134 which was filed 5/8/95.

The technology for inserting digital watermarks in images and the technology for reading or detecting digital watermarks in images is well developed, well known and described in detail in public literature. Furthermore, there are commercially available products which include programs or mechanisms for inserting digital watermarks into images. For example the commercially available and widely used products "Adobe Photoshop" which is marketed by Adobe Corporation of San Jose California and "Corel Draw" program which is marked by Corel Corporation of Ontario Canada, include a facility for inserting digital watermarks into images.

The technology for making high quality copies of documents is widely available. The technical quality of scanners and color printers has been increasing rapidly. Today for a relatively low cost one can purchase a high quality scanner and a high quality color printer. Thus, it is becoming increasingly easy to duplicate documents. The ability to create high quality copies has created a need for technology which can differentiate between original documents and copies of the original.

It is known that watermarks can be used to help differentiate genuine documents from copies. However, the prior art techniques for using digital watermarks to differentiate genuine documents from copies have serious limitations. The present invention is directed to an improved technique for using steganography

and digital watermark technology to facilitate differentiating original documents from copies of the original.

The present invention can also be used for various other purposes such as to embed multiple types of information in a single document or to provide watermarks that enable documents to perform special functions. .

Summary of the Invention

With the present invention multiple digital watermarks, each of which has a different character, are embedded in a document. The characters of the two watermarks are chosen so that the watermarks will be affected in different manners by what may subsequently happen to the document.

The detection process or mechanism reads the two digital watermarks and compares their characteristics. While wear and handling may change the characteristics of the individual watermarks, the relationship between the characteristic of the two watermarks will never-the-less give an indication as to whether a document is an original or a copy of an original.

For example according to the present invention two digital watermarks in a document may have different energy levels. The absolute energy level of a digital watermark in an original image may be decreased if a document is subject to wear. Likewise the energy level of the digital watermark in an image may be decreased if an image is scanned and reprinted on a color printer. However, the relationship between the energy level of the two digital watermarks will be different in an image that has been subject to wear and in a reproduced image. Likewise if two digital watermarks are introduced into an image where the bit pattern used to construct the digital watermarks have different patterns, the ratio between the signal to noise ratio of the watermarks will be different in an original subject to wear and in a copy generated by scanning the original and printing the scanned image. Other characteristics of multiple digital watermarks can also be used to differentiate original documents from copies.

In other embodiments, a watermark-independent assessment of wear can be performed, and the results used to aid in differentiating original documents from copies.

Brief Description of the Figures

Figure 1 shows the paths that a document and a copy may follow.

Figures 2A and 2B show a fine grain and a course grain watermark.

Figure 3A and 3B show a geometrically linear and a geometrically random assignment of pixels to a bit in a digital watermark.

Figure 4 illustrates a fourth embodiment of the invention.

Detailed Description

The problem of differentiating an original document from a copy is made more difficult in situations where the original document is subject to being handled, worn, folded and otherwise damaged. Many original documents such as identification documents and currency are extensively handled. The wear to which such documents is subjected reduces the quality of images on the document and therefore reduces the quality of any information embedded in the document using conventional steganographic techniques.

With the present invention, a number of different watermarks are embedded in a document. Each of the watermarks embedded in the document has a different character. All watermarks are somewhat affected when a document is subjected to wear, and all watermarks are somewhat affected when a document is duplicated by being scanned and reprinted. However, the magnitude of the effect caused by being scanned and reprinted on watermarks with certain characteristics is much greater than the effect on watermarks with different characteristics. Likewise, wear and handling of a document affects watermarks with certain characteristics much more than it affects watermarks with different characteristics.

Thus, if multiple watermarks with different characteristics are inserted into a document, it is possible to differentiate a copy from an original document that has been subjected to wear by examining the ratios of characteristics of the watermarks in the image being examined.

In order to print a document on a color printer, the document is put through a transformation from a color space such as the RGB color space to a different color space such as the CMYK (cyan, magenta, yellow, black) color space. Such transformations are well known. For example see chapter 3 entitled "Color Spaces" in a book entitled "Video Demystified, A handbook for the Digital Engineer," Second Edition, by Keith Jack, published by Harris Semiconductor/ Hightext Publications of San Diego, California, and "The Color PC" by Marc Miller and published by the Hayden Press.

When an image is transformed from one color space to another color space, noise is introduced into the image. Among the reasons for this is the fact that each color space has its own distinctive gamut (or range) of colors. Where the gamut of two color spaces overlap, the conversion from one color space to another color space can in theory be precise. However, there will be some areas that are in the gamut of one color space but not in the gamut of another color space. Such situations definitely introduce noise into the conversion process. Even in areas that are in the gamut of two color spaces, conversion from one color

space to another color space introduces noise because of such things as round off errors. The present invention takes advantage of the fact that if an original is copied and then a copy is printed, the image on the printed copy will have gone through several conversions to which the original will not have been subjected. For example, the conversions to which a copy may be subjected are:

1) a document to RGB conversion (i.e. scanning the document into the computer),

2) a RGB to CMYK conversion,

3) a CMYK to copy conversion (i.e. printing the document).

Any characteristics of the two digital watermarks that will be affected differently by the additional conversion process to which copies are subjected can be used to differentiate copies from an original. Since the two watermarks with different characteristics are affected in a different manner by the additional conversion step, a comparison of the characteristics of the two watermarks in a document being examined will indicate if the document is an original (which has not gone through the additional conversions) or a copy which has gone through the additional conversions. While the characteristics of each watermark will have been changed by wear and by the copying process, the comparison between the characteristics of the two watermarks will still be able to differential a copy from an original.

Four embodiments of the invention are described below. Each of the embodiments utilizes two watermarks in a document. The differences between the two watermarks in the document are as follows:

In the first embodiment:

First watermark: Has fine grain

Second watermark: Has a course grain

In the second embodiment:

First watermark: Has geometrically linear assignment of pixels

Second watermark: Has geometrically random assignment of pixels.

In the third embodiment:

First watermark: Has low power

Second watermark: Has higher power

In the fourth embodiment:

First watermark: uses standard RGB to HSI and HSI to RGB transformations

Second watermark is biased before being transformed from HSI to RGB.

Figure 1 shows the steps to which documents and copies are typically subjected. In the normal course, a document 10 may be subjected to handling and wear 11 resulting in a worn document 10A. Document 10 may also be scanned as illustrated by box 12. The scanning produces a digital image that can be printed, as illustrated by box 13. The printed image may be subjected to handling and wear 14 resulting in a copy 10B. It is noted that the document 10 may also be subject to handling and wear prior to the scanning

operation 12. The task to which this invention is directed is the task of differentiating the worn document 10A from the copy 10B.

The document 10 includes an image (not explicitly shown) that has two digital watermarks inserted therein. In the first embodiment of the invention, the first watermark has a fine grain and the second watermark has a course grain. The grain of the two watermarks is illustrated in Figure 2. Figure 2A shows the grain of the first watermark and figure 2B shows the grain of the second watermark. The first watermark uses blocks of 9 pixels (a 3 by 3 block). Each of the pixels in each 9 pixel block has its gray value changed by the same amount. For example Figure 2A shows that the first 9 pixel block has its gray value increase and the second 9 pixel block has its gray value decreased. The amount of increase and the selection of blocks that is increased and decreased is conventional.

As shown in Figure 2B, the grain of the second watermark is in blocks that are 6 pixels by 6 pixels or 36 pixels. All of the pixels in each 36 pixel block are changed by the same amount.

In the original document 10, the two watermarks have power ratios of 1 to 1. After wear and handling, the power of the first watermark will be degraded somewhat more than the power of the second watermark. For example, as illustrated in Figure 1, after document 10 is subjected to handling and wear, a detector which reads the watermarks might find that the power ratio of the water marks is 1 to 2.

If the document 10 is scanned and the resulting digital image is printed to make a copy of the document 10, the ratio of the power of the watermarks will be affected much more than the effect of handling and wear. For example as illustrated in Figure 1, the power ratio of the watermarks may be 1 to 10, thereby allowing one to differentiate the worn original document 10A from the copy 10B.

It is noted that the mechanism for inserting watermarks into an image is well known, as is the technique for reading a watermark and using correlation techniques to determine the signal to noise ratio (i.e. the power) of a watermark.

Figures 3A and 3B show an alternative technique for implementing the present invention. In the second embodiment of the invention, the two watermarks inserted into the image on a document have different patterns of assigning pixels to the bits of the payload represented by the watermark. The first watermark utilizes a geometrically linear assignment of pixels to each bit. For example Figure 3A shows an image that has 500 by 500 pixels. Considering a watermark payload with 50 bits, each bit of the watermark would have 5000 pixels assigned to represent that bit. A linear assignment could have each fifth bit in each

row (100 bits per row) and each fifth row (50 rows) assigned to each bit of the watermark. Thus 5000 pixels would be assigned to each bit in a very orderly or linear manner.

In the second watermark the pixels would be assigned to each bit in a random manner as shown in Figure 3B. Each bit in the watermark would still have 5000 assigned bits; however, the pixels would be a random location over the image. Naturally it should be understood that Figure 3A and 3B illustrate how pixels are assigned to one bit of the watermark. The other bits of the watermarks would have pixels assigned in a similar manner.

Similar to the first embodiment of the invention, the watermark with a linear assignment of pixels and the watermark with a random assignment of pixels would be affected differently by handling and wear on the original document than they would be by being scanned and reprinted.

The third embodiment of the invention described herein utilizes watermarks that have different power levels. Handling and wear as contrasted to scanning and printing would affect a watermark with a low power level differently than a watermark with a high power level. Watermarks with different power levels can be inserted into a document in order to practice the present invention utilizing commercially available programs such as Adobe Photoshop or Corel Draw. In the Adobe Photoshop and Corel Draw programs, the power or intensity of the watermark can be adjusted by setting a simple control setting in the program.

The fourth embodiment of the invention introduces different characteristics into two watermarks by modifications made to one of the watermarks during the initial step during which the watermarks are introduced into an image. The operation of the fourth embodiment can be explained as shown in Figure 4. First as illustrated by equation 1 there is a conversion from RGB to HSI as is conventional. This is illustrated by equation 1. As illustrated by equation 2, the first watermark is inserted into the image in a conventional manner by modifying the I value in the HSI representation of the image using the first watermark values (designated as WM1 Δ). A first RGB value designated RGB(1) is then calculated using a conventional transformation designated T. As indicated by equation 3, the second watermark WM2 is then biased toward a particular color and the biased watermark is then combined with the HSI values and transformed to a second set of RGB values designated RGB(2). Finally as indicated by equation 4, the values RGB(1) and RGB(2) are combined to form the watermarked image designated RGB(F).

The transform used to go from RGB to HSI color space (indicated in equation 1 in Figure 4) can be anyone of a variety of known other techniques. For example, the RGB to HSI conversion can be one of the techniques explained in the above referenced text book such as the following: (which assumes that RGB and Intensity have a value range of 0 to I and that Red equals 0°):

First calculate:

$M = max (R,G,B)$

$m = min (R,G,B)$

$r = (M-R)/(M-m)$

$g = (M-G) /M-n)$

$b = (M-B) / (M-m)$

Then calculate I, S, and H as follows:

a) $I = (M + M) /2$

b) if $M = m$ *then* $S = 0$ *and* $H = 180$

if $I <$ *or* $= 0.5$ *then* $S = (M-m)/(M+m)$

if $I > 0.5$ *then* $S = (M-m) / (2-M-m)$

c) if $R = M$ *then* $H = 60 (b-g)$

if $G = M$ *then* $H = 60 (2 + r - b)$

if $B = M$ *then* $H = 60(4 + g - r)$

if $H >$ *or* $= 360$ *then* $H = H - 360$

if $H < 0$ *then* $H = H + 360$

The first watermark in inserted into the RGB values in a conventional manner by modifying the I value of appropriate pixels so as to combine the watermark Δ values with HSI values. This is indicated by equation 2 in Figure 4. Next as indicated by equation 3 in Figure 4, the HSI values are converted to RGB values using a transform "T". The transform "T" can be conventional and it can for example be done as follows:

First calculate:

if $I <$ *or* $= 0.5$ *then* $M = I (I + S)$

if $I > 0.5$ *then* $M = I + S - IS$

$m = 2I - M$

if $S = 0$ *then* $R = G = B = I$ *and* $H = 180°$

Then calculate R, G and B as follows:

a) if $H < 60$ *then* $R = M$

if $H < 120$ *then* $R = m + ((M-m) / ((120- H) / 60))$

if $H < 240$ *then* $R = m$

if $H < 300$ *then* $R = m + ((M - m) / ((H - 240 / 60))$

otherwise $R = M$

b) if $H < 60$ *then* $G = m + ((M-m)/ (H/60))$

if $H < 180$ *then* $G = M$

if $H < 240$ *then* $G = m + ((M - m) / ((240 - H\_ / 60))$

otherwise $G = m$

c) if H < 120 then B = m

if H < 180 then B = m + ((M -m) / ((H-120/60))

if H < 300 then B = M

otherwise B = m + ((M - m) / ((360 - H) / 60))

Next the values which represent a second watermark are used to calculate a second set of RGB values designated RGB2. In order to calculate RGB2, the values of H and S are modified so that they are slightly biased toward a particular color designated H1 and S1 New values for H and S are calculated as follows: (Note, H1 must be between 0 and 360, S1 must be non-negative and can be between 0 and 1 and X is a value between 0 and 1)

Calculate new values for H and S as follows:

If H > H1 then H = H - (H - H1) x

else H = H + (H1 -H)x

If S > S1 then S= S - (S- S1)x

else S = S +(S1 -S) x

:

Next add the second watermark to the values of HSI and transform these values to the RGB color space as indicated by equation 3 The transformation from HSI color space to RGB color space is done as previously indicated.

Finally as indicated by equation 4 in Figure 4, the final RGB value (designated RGBF) is calculated by combining the values of RGB1 and RGB2. This combination can be done in a variety of known ways.

It is noted that in the above example the difference between the transformation used for the first and the second watermarks involves biasing the values of H and S. Alternatively a wide variety of different changes could also be made. The key to this fourth embodiment of the invention is that in effect a different transformation is used for the first and the second watermarks.

In more sophisticated embodiments, the wear of the document can be independently assessed and used to aid in distinguishing an original from a copy.

There may be cases in which the wear-based degradation to the watermarks in a worn but original document can yield results similar to the scan/print degradation to the watermarks in a crisp copy. For example, consider the case of an original document having watermarks A and B of equal energy, but tailored so that watermark B is more frail and falls-off rapidly in energy when photocopied. On finding a suspect document with a ratio of energy between the two documents in excess of 2:1 (or a commensurate

difference in signal-to-noise ratios), a counterfeit may be presumed. However, this ratio may also result from extreme wear of an original document. See, e.g., the watermark strength v. wear chart of Figs. 5A and 5B for an original document, and the same document after scanning on a 600dpi scanner and printing on a 720 dpi printer. The original document degrades to a watermark energy ratio of 2:1 at point x. A crisp copy has the same ratio, resulting in a potential ambiguity.

To distinguish these two cases, the wear of the document can be assessed. Various means can be used to distinguish document wear. One is high frequency content, as can be determined by high pass filtering the document image data, or performing an FFT, DCT, etc. A worn document typically loses some high frequency energy. Another is contrast - a worn document typically loses contrast. Still another is color gamut – a worn document may fade to a less varied gamut. Still another is luminance – the soiling of a document can decrease the overall document brightness. Yet another is physical integrity – a worn document droops when only partially supported. Yet another means is a quick human assessment of wear, with human entry of a corresponding datum into a system (e.g., on a wear scale of 0 to 10, or simply "crisp," "used," or "very worn"). Still other means can similarly be employed.

The wear can be graded on an arbitrary scale, depending on the particular measurement means used. In an illustrative case, wear may range from 0 ("crisp") to 7(extreme). In the Fig. 5 example, the x point may be at wear value 5. In distinguishing the documents, a look-up table, microprocessor-implemented algorithm, or other arrangement can be provided that takes as its input the ratio and wear values, and produces outputs, e.g., as follows:

	Wear=0	*Wear=1*	*Wear=2*	*Wear=3*	*Wear=4*	*Wear=5*	*Wear=6*	*Wear=7*
Ratio = 1.0	*Original*	*Original*	*Original*	*Original*	*Error?*	*Error?*	*Error?*	*Error?*
Ratio = 1.25	*Original*	*Original*	*Original*	*Original*	*Original*	*Error?*	*Error?*	*Error?*
Ratio = 1.5	*Original*	*Original*	*Original*	*Original*	*Original*	*Original*	*Error?*	*Error?*
Ratio = 1.75	*Copy*	*Copy*	*Original*	*Original*	*Original*	*Original*	*Original*	*Error?*
Ratio = 2.0	*Copy*	*Copy*	*Copy*	*Copy*	*Original*	*Original*	*Original*	*Original*
Ratio = 2.25	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Original*	*Original*	*Original*
Ratio = 2.5	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Original*	*Original*

Ratio = 2.75	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Original*	*Original*
Ratio = 3.0	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Original*
Ratio => 3.25	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*	*Copy*

(The "Error?" outputs corresponds to cases that should not occur in actual practice, e.g., a very worn document in which the ratio of watermarks is 1.0.)

While four embodiments and a further enhancement of the invention have been shown herein, it should be understood that many other characteristics and attributes of a digital watermark could be used to practice the present invention in addition to the characteristics and attributes described herein. Furthermore other known digital watermarking techniques can be used together with and applied to the digital watermarks used for the present invention. It is also noted that while in the above examples only two watermarks were used; in some situations one could use three, four five or more watermarks. That is, the embodiments of the invention specifically described herein utilize two watermarks. It should be understood that any number of watermarks could be utilized in like manner. Furthermore while the embodiments shown herein utilize two separate watermarks, the two watermarks used to practice the present invention could be combined into one watermark which has a plurality of separate identifiable and measurable characteristics.

Still further, while the invention was particularly illustrated with reference to watermarking that is effected in the pixel domain, the same techniques are likewise applicable to watermarking effected in the DCT, wavelet, or other domain (e.g., as shown in US Patent 5,930,369). Moreover, some documents may include watermarks effected in two different domains (e.g., pixel and DCT).

Still further, the different watermarks can be of entirely different types. For example, one watermark can comprise slight alterations to the image normally printed on a document, and the second can comprise a texture formed on the document substrate, or a background weave or tint pattern – both of which convey watermark data. (Examples of texture-, weave- and tint-based watermarks are shown, e.g., in copending applications 09/074,034 (filed May 6, 1998), 09/127,502 (filed July 31, 1998), 09/151,492 (filed September 11, 1998), patent 5,850,481, and laid-open PCT publication WO 99/53428.

It is noted that while the present invention utilizes multiple watermarks with different characteristics to differentiate original documents from copies of the original, one can also utilizes multiple watermarks with

different characteristics for other reasons. Documents may include multiple similar watermarks in addition to the watermarks having different characteristics according to the present invention. As used herein, the term "document" generally refers to a physical entity. However, the same methodologies can also be applied to purely digital images – e.g., to detect losses that an image has suffered through a lossy compression/decompression process such as JPEG or MPEG, color re-balancing, etc., and thereby discern something about the history of a digital image.

It will be recognized that the principles of the invention can be incorporated into an apparatus used at cash registers and other points of sale to assess the genuineness of banknotes, food stamps, coupons, and other documents. Such an apparatus can include a scanning 1D, or stationary 2D image sensor (e.g., CMOS or CCD), and a microprocessor suitably programmed to discern first and second watermarks in image data provided by the sensor (as well as wear, if desired). (In some cases, a stationary 1D sensor may be employed.) Such apparatus further includes an output device - such as a display screen, indicator light, audible tone, voice synthesizer, or equivalent device - to provide an appraisal of the document's validity based on the sensed information.

A similar apparatus can be provided for use by Customs officials at ports of entry to check merchandise tags, packaging, labels, and other printed indicia associated with clothing, purses, electronic components, software, and other readily-counterfeitable goods, to determine whether the sensed tag/package/label is an original, or a copy. While such a determination may not provide the confidence needed to seize a shipment as counterfeit, it could flag the goods as suspect and needing further inspection and/or forensic analysis.

The idea in each of the foregoing apparatuses is, of course, to provide an indication of possible non-genuineness more reliable than the typical casual and semi-casual human inspection during very fast point-of-sale transactions and other similar high traffic volume situations, where it is unrealistic to expect human observation to be efficient "flaggers" of suspect product and documents.

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the documents (including applications) cited above.

While the present invention has been described with respect to four specific embodiments of the invention, it should be understood that various changes in forma and detail could be made without departing from the spirit and scope of the invention. The scope of the present invention is limited only by the appended claims.

We Claim

1. A method comprising:

sensing a first parameter related to a first watermark in a document;

sensing a second parameter related to a second watermark in the document;

sensing a third parameter related to wear of the document; and

by reference to said first, second and third parameters, assessing whether the document is likely an original document.

2. A method comprising:

step for sensing data from a printed object; and

step for determining whether the printed object is likely an original.

3. Apparatus comprising:

means for producing image data corresponding to a printed object; and

means for assessing whether the printed object is likely an original.

4. A document including a substrate with printing thereon, the printing encoding at least first and second steganographic watermarks.

5. The document of claim 4 where the document is one of the group consisting of a product label, a product tag, product packaging, a banknote, a coupon, and a food stamp.

6. The document of claim 4 in which the first and second watermarks are designed to change differently when the document is subjected to first and second corruption processes.

7. The document of claim 6 in which the first corruption process includes wear, and the second corruption process includes scanning and printing.

METHODS AND SYSTEMS USING MULTIPLE WATERMARKS

Abstract of the Disclosure

Two or more digital watermarks, with different characteristics, are embedded in a document. The characteristics are chosen so that the watermarks will be affected in different manners if the document is subsequently copied or reproduced. The detection process or mechanism reads two or more of the watermarks and compares their characteristics. While wear and handling may change the characteristics of the digital watermarks in a document, the relationship between the characteristics of the multiple digital watermarks in a document will nevertheless give an indication as to whether a document is an original or a copy of an original. Document wear can be independently assessed and used as an aid in interpreting the detected watermark characteristics.

APPENDIX D

Image Patterns that Constitute Digital Watermarks

The present application is a continuation of *:*

Co-pending application serial number 60/131,005 filed April 22, 1999.

Field of the Invention:

The present invention relates to steganography and more particularly to digital images that contain digital watermark data.

Background of the Invention:

Steganographic techniques for unobtrusively embedding digital data in images are well known . For example, widely used image editing programs such as Adobe PhotoShop which is marketed by Adobe Corporation, CorelPHOTOPAINT which is marketed by Corel Corporation, and Microgrfix Webtricity which is marketed by Micrographic Corporation contain plug-ins or subroutines which can add watermarks to images and which can read watermarks. Systems for adding watermarks to images are described in many patents including U.S. patent 5,636,292, U.S. patent 5,862,260, and U.S. patent 5,748,783. Such systems are also described in the technical literature such as in the "Communications of the ACM" published July 1998 Vol. 41, No 7 pages 31 to 77. The teaching and information in the above referenced prior material is hereby incorporated herein as background information.

In general in watermark detecting and reading systems the original image is considered to be noise when the system is detecting and reading the actual watermark data. A major task faced by the designers of watermark reading systems is how to detect a relatively weak watermark signal in view of the noise signal created by the image data itself.

Many documents and images include a background image. In some documents such as checks, passports, etc. the background image is used as a security feature to inhibit alteration or duplication. In many documents, the background consists of a series of lines. Such lines are designed to both present a pleasing appearance and to inhibit duplication or alteration of the documents. Co-pending US patent applications 09/074,034, filed May 6, 1998 and 09/127,503, filed July 31, 1998 (which correspond to PCT/US99/08252, now published as WO99_____ and PCT/US99/14532) describe how the width of lines can be varied to carry a watermark.

Prior art watermarking technology modifies an image by changing the luminance values of the pixels in the image in such a way that the modified image carries digital data (referred to as watermark payload data). As shown in Figure 1, the prior art watermarking systems begin with an image 10 and watermark payload data 14. A watermarking program 11 calculates a luminance change value 12 for each pixel in a watermark tile. The input image is divided into areas corresponding to the size of the watermark tile. A modified image is generated by taking the luminance values in each area of the original image and changing it by an amount equal to the change values in the corresponding position in the watermark tile. Watermark detecting and reading program 14 can read the watermark payload data by detecting the changes in luminance values while considering the values from the original image as "noise". Watermark detecting and reading program 14 can read the payload data not withstanding changes in scale and rotation of the modified image. Such a system is for example shown in co-pending patent application serial number SN 09/503,881 filed February 14, 2000 (the material in which is hereby incorporated herein by reference).

Summary of the Present invention:

The present invention is directed to designing a pattern of lines in such a manner that the pattern itself carries watermark payload data. That is, with the present invention lines are drawn so that the resulting image carries watermark data. This is in contrast to the prior art where watermark payload data is used to modify a preexisting image. With the present invention, a conventional watermarking program is used to calculate luminance change values in a watermark tile (i.e. luminance change values corresponding to a desired watermark payload). The luminance change values are used to control the formation of lines on an output image. The weight, length and character (i.e. straight or wavy etc.) of the lines can be selected to create any desired aesthetic effect so long as the placement of the lines is controlled by the luminance change values in the watermark tile. With the present invention lines are drawn to form an image in such a way that the placement and direction of the lines that carries watermark data. The payload data can be read from an image created according to the present invention using a conventional watermark reading program.

With the present invention as a first step, the luminance change values in a watermark tile are calculated using a watermarking program. Next the values so calculated are quantified into a relative small number of levels. For example, the watermarking change values calculated by the watermarking program may have 256 different values (0 to 255). The present invention takes those values and quantify them into ten different levels. An output image is divided into relatively large areas (called bumps), one bump for each pixel in the watermark payload tile. For example, each bump area in the output image could be one hundred pixels by one hundred pixels. Each bump area in the output is given an index value corresponding to the luminance change value of the corresponding pixel in the payload tile area. Starting at an arbitrary

bump area in the output image, a line is drawn to the surrounding bump area with the highest index value and the index value of the bump area where the line started is decreased by one. The process then repeats from the bump area where the line ended. The process can stop when all bump area have reached an index value of zero, or sooner if a less robust watermark is acceptable.

Brief Description of the drawings:

Figure 1 shows a prior art watermarking system.

Figure 2 is an overall system diagram of the present invention.

Figure 3 illustrates the correspondence between the luminance values in a watermark tile and areas in the output image.

Figure 4 is a flow diagram of the present invention.

Figure 5 shows the lines in an output image.

Figure 6 shows an alternative arrangement of lines in an output image.

Figure 7 is an overall diagram of an output image.

Detailed Description:

The present invention takes the luminance change values in a watermark tile that are calculated by a prior art watermarking program and uses these values to control the construction of lines on an output image. The calculation of the luminance change values is not part of the present invention and these values may be calculated using prior art watermarking programs. For example, the luminance change values can be calculated as described in patent application serial number SN 09/503,881 filed February 14, 2000 which is hereby incorporated herein by reference. It is noted that in many prior art systems the watermark data (i.e. the watermark tile) is replicated many times over an image. The first embodiment of the invention described herein does not duplicate or replicate the watermark data in the output image; however, as explained later in other embodiments of the invention the watermark data can be replicated in multiple patterns. The present invention relates only to the construction of an image carrying watermark payload data. The watermark payload data can be read from the output image using a conventional prior art watermark reading program.

As shown in Figure 2, a preferred embodiment of the present invention utilizes a watermarking program 11 to calculate luminance change values 12 for each pixel in a watermark tile. The luminance change values 12 in the watermark tile corresponding to a particular watermark payload 14. With the present invention the original image (herein called a pseudo image) presented to the watermarking program 12 can be a uniformly gray image 10A, that is, an image which has a selected luminance value which is uniform over the entire image. The embodiment described here only uses a pseudo image 10A for the convenience since conventional watermarking programs begin with an image. The effect is the same as if

there were no image. In alternate embodiments, the watermark change values 12 could be calculated directly without need for a pseudo image 10A.

The luminance change values in a watermark tile calculated by prior art watermarking program 11 has 256 (0 to 255) luminance levels. To simplify operation of the system, with the present invention these values are quantified into a much smaller number of levels. For example, the 256 levels can be quantified into ten levels as indicated by box 22 in Figure 2. The number of levels used (and in fact whether or not there is any reduction in the number of levels) is determined by the degree of complexity one is willing to have in the program. One could use all the levels in the normal watermark tile; however, such a program would require much more time to generate a pattern. Alternately, one could design a watermarking program that only generates ten change values. Such a program would in effect be simpler than the watermarking programs now in commercial programs such as those previously referenced.

One must choose the characteristics of the lines one wants to use. A significant advantage of the present invention is that the characteristics of the lines can be chosen for aesthetic reasons. For purposes of simplicity of illustration, the lines chosen for the illustrative example shown herein are straight and which have a weight of 4 points. Alternative embodiments can use may different types of lines as explained later.

As shown in Figure 3, the present invention uses a watermark tile 30 created by a watermarking program 11. The luminance change values in the watermark tile 30 are used to control the drawings of lines in an output image 35. For convenience and clarity of illustration only five pixels 3A to 3E are illustrated in Figure 3. It should be understood that the watermark tile has many more pixels than shown. For example, a watermark tile generated by a conventional watermarking program has over one thousand pixels. The particular and exact size of the watermark tile is of no particular significance to the present invention; however, it does affect the number of areas in the output image.

The output image is divided into areas or bumps as shown in Figure 3. For reference the areas or bumps that are illustrated in Figure 3 are designated as 4A, 4B, 4C, 4D and 4E. Each area can for example be 100 pixels by 100 pixels. The arrows 31A and 31B in Figure 3 illustrate that the output image has many more area than the five areas 4A to 4E explicitly shown in Figure 3. There is one area in output image 31 for each pixel in watermark tile 30.

The luminance change values in watermark tile 30 are first quantified into ten levels as indicated by block 22 in Figure 2. It is noted that in the preferred embodiment the luminance change values in watermark tile 30 are generated by a conventional watermarking program, have luminance change values that range from 0 to 255. It is difficult to deal with that many levels with the present algorithm and it has been found that

satisfactory results can be obtained by quantifying the values into many less levels. For example, in preferred embodiment, the luminance values in the watermark tile are quantified into ten levels. That is, the values from 0 to 255 are divided into ten levels and each pixel is assigned an index value depending upon which range its luminance change value. (it is noted that the number ten is arbitrary and more or less levels can be selected to meet the needs of a particular embodiment).

The output image has one area (or bump) for each pixel in the watermark tile and each area in the output image corresponds to one pixel in the watermark tile. The index value calculated for each pixel in the watermark tile is assigned to the corresponding area in the output image. Figure 5 shows the areas in output image 31 in additional detail. In Figure 5, the areas are referenced using a conventional matrix notation. For example area 4A is designated as area 1,1, area 4B is designated area 1,2 etc. The starting index value for each area is the index value for the corresponding pixel in the watermark tile. The starting index value for each area is given by the number in bold type in Figure 5.

The characteristics of the lines in the output must be chosen as indicated by block 23 in Figure 2. For purposes simplicity, the example described here utilizes lines that are straight with a weight of four pixels. However, depending upon the artistic effect desired, lines with a wide range of characteristics can be chosen. For example lines that have waves at selected frequencies can be used. Dotted lines can be used. Very thin lines or very heavy lines can be used. Lines that are tapered in width can be used. The above are merely a few examples of the types of lines that can be used to achieve desired artistic effects. However, for ease of illustration in the example explained here straight lines with a weight of four pixels are used.

Lines are drawn in the output image using the algorithm shown in Figure 4. First, a starting point is picked as indicated by block 44. For purposes of the example described here area 1,1 is chosen as the starting point. It is however, noted that the location of the starting point can be chosen arbitrarily. Next as indicated by block 42, the index values of the area adjacent to the starting area are examined and the area with the highest index value is selected. In the present example, there are only two adjacent area, namely areas 1,2 and 2,1. Area 1,2 has an index value of 5 and area 2,1 has an index value of 2. A line is drawn from the starting area to the adjacent area with the highest index value as indicated by block 43. In this case area 1,2 is the adjacent area with the highest index value. The starting location of the line can be chosen randomly. For simplicity in the present embodiment lines are drawn only horizontally or vertically; however, in alternative embodiments lines can be drawn at angles selected randomly or according to any desired pattern. The length of the lines can be chosen randomly so long as a line begins and ends in the designated area.

After a line is drawn from one square to another square, the index value of the square where the line started is decreased by one as indicated by block 45. This is shown in Figure 5 by the numbers in parenthesis. Hence for the line described above, the index value for area 1,1 is reduced from 4 to 3. The process then repeats. Area 1,3 is the area adjacent to area 1,2 that has the high index value (excluding the area where the line to area 1,2 originated). A line is therefore drawn from area 1,2 to area 1,3 and the index value of area 1,2 is reduced from 5 to 4. Following the same algorithm a line is next drawn to area 2,3 and then a line is drawn to area 3,2.

The process can continues until all areas have an index of zero. However, it has been found that the process can be stopped after the number of lines drawn equals the number of squares. Other criteria can be used to determine when to stop the process. Basically, by trial and error one can determine when a watermark with sufficient intensity has been embedded in the image or when the desired artistic effect has been achieved. If prior to the time one cares to terminate the process, one arrives at a point where all the adjacent areas have an index value of zero, one can merely restart the process from an arbitrary location. Likewise if one arrives at a point where all the adjacent area have the same index value, one can arbitrarily choose where to draw a line.

In the embodiment shown, the lines begin at random locations. Figure 6 shows an example where each line begins from the terminal point of the previous line. Again here the length of the lines is chosen randomly.

In the embodiment shown above, lines are drawn between area in the output image. It is noted that artifacts other than lines could be used. For example, instead of lines, one could use circles, or stars, or small images of birds. In fact one can use any artifact that would create a change in luminance which could be detected by a watermark reading program.

Conventional watermarking program redundantly encode the watermark data in an image. This increases reliability and robustness of the watermark. Likewise with the present invention, a pattern could be repeated in an output image. The repeated pattern could be the same pattern or it could be a different pattern carrying the same watermark. That is, one could have multiple identical patterns in an output image. Alternatively, one could have multiple pattern which differ from each other but which carry the same watermark payload data. For example, different patterns can be generated by merely starting the process at a different location in the image. Alternatively, one could have different patterns using different types of lines, or for example patterns where the starting are for the line drawing algorithm was at a different area in the output image. The size of the areas or bumps in the output image have the same affect as do the size of the areas or bumps in an image modified by a conventional watermarking program.

While the invention has been shown and described with respect to preferred embodiments thereof, it should be understood that various changes in forma and detail can be made without departing from the spirit and scope of the invention.

I claim:

1. A method of generating a watermarked image, said image being divided into a plurality of areas, said method comprising the steps of
generating a watermark tile which contains luminance change value for pixels which will embed a watermark in an image,
associating said areas in said image with pixels in said watermark tile,
drawing lines between said areas in said output image, the beginning and end of said lines being dependent at least in part on the luminance change values of the pixels in the watermark tile that correspond to the area where said lines begin and end.

2. An physical image which contains a plurality of lines, said image being divided into a plurality of areas, said image being created by lines drawn between said areas so as to carry a digital watermark payload.

3. A system for creating an image which carries a watermark payload, said system comprising,
means to generate a watermark tile containing luminance change values that represent a watermark payload,
means for drawing lines in an image in response to the change values in said watermark tile, whereby said image carries a watermark payload.

4. The method recited in claim 1 where said areas each have an index value that is related to the change value of the associated pixel in said watermark tile.

5. The method in claim 4 where each line is drawn from an area to an adjacent area which has the highest index value.

6. An physical image which contains a plurality of artifacts, said artifacts being created at selected positioned so as to carry a digital watermark payload.

7. An physical image which contains a plurality of visual objects said visual objects being created at selected positioned so as to carry a digital watermark payload.

8. A system for generating a watermarked image, said image being divided into a plurality of areas, said method comprising,

a program for generating a watermark tile which contains luminance change value for pixels which will embed a watermark in an image,
areas in said image being associated with a pixels in said watermark tile,
a program for drawing lines between said areas in said output image, the beginning and end of said lines being dependent at least in part on the luminance change values of the pixels in the watermark tile that correspond to the area where said lines begin and end.

9. A method of drawing an image which contains a watermark payload, said image being divided into a plurality of areas,
generating a watermark tile which specifies luminance change value which will represent a watermark payload,
drawing lines between areas in said image in response to the values in said watermark tile.

10. The method in claim 10 wherein said watermark tile has change values for a plurality of pixels, and wherein said image contains at least as many area as there pixels in said watermark tile.

11. The method in claim 11 wherein the lines drawn between each area depends upon the change value in the corresponding pixel in said watermark tile.

12. The method in claim 11 wherein the change values in said watermark tile are grouped into a number of groups before said lines are drawn.

13. The method of claim 12 wherein said change values are grouped into ten groups.

14. A method of drawing an image in response to change values in a watermark tile generated by a watermarking program, said watermark tile having change values for a particular number of pixels which represent a particular payload,
grouping said change values into a selected number of groups,
dividing said image into bump areas, each bump area being associated with one pixel change value in said watermark tile, each bump area having an index value directly related to the associated pixel change value in said watermark tile,
starting to draw lines in said image at a selected bump area by drawing a line from said selected bump area to the adjacent bump area having the highest index value,
decreasing the index value of the bump area where said line started,

drawing another line from the bump area where said first line terminated to the adjacent area having the highest index value, and

repeating said decreasing and said drawing another line step for a selected number of iterations, whereby a watermark reading program can read said particular payload from said image.

Abstract

The present invention is directed to designing a pattern of lines in such a manner that the pattern itself carries watermark payload data. That is, with the present invention the lines are drawn so that the resulting image carries watermark data. This is in contrast to the prior art where watermark payload data is used to modify a preexisting image. With the present invention, a conventional watermarking program is used to calculate luminance change values in a watermark tile (i.e. luminance change values corresponding to a desired watermark payload). The luminance change values are used to control the formation of lines on an output image. The weight, length and character (i.e. straight or wavy etc.) of the lines can be selected to create any desired aesthetic effect so long as the placement of the lines is controlled by the luminance change values in the watermark tile. With the present invention lines are drawn to form an image in such a way that the placement and direction of the lines that carries watermark data. The payload data can be read from an image created according to the present invention using a conventional watermark reading program.

APPENDIX E

METHODS AND SYSTEMS FOR DIGITAL WATERMARKING

Related Application Data

The present application is related to copending applications 09/127,502, filed July 31, 1998; 09/074,034, filed May 6, 1998; 09/234,780, filed 1/20/99; 09/433,104, filed November 3, 1999; 09/503,881, filed February 14, 2000; and application _____, filed April 20, 2000, entitled Image Patterns that Constitute Digital Watermarks.

The present application is also related to applications entitled Digital Watermarking of Physical Objects, and Digital Watermarking Systems, both filed herewith.

The present application is also related to the assignee's patents 5,862,260, 5,850,481and 5,841,886.

Field of the Invention

The present invention relates to processing of physical media (e.g., blank printing stock, product packaging, catalogs, advertisements, etc.) to impart a machine-readable indicia (e.g., a plural-bit digital watermark) thereto.

Background and Summary of the Invention

Digital watermarking technology, a form of steganography, encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration.

Most commonly, digital watermarking is applied to digital objects, such as digital image, video, and audio. In the case of images, slight changes can be made to local luminance or color values to effect the encoding. These changes can later be detected by a computer, and analyzed to discern the watermark information represented thereby.

Digital watermarking techniques can also be applied to traditional physical objects, including blank paper. Such blank media, however, presents certain challenges since there is no image that can serve as the carrier for the watermark signal.

The assignee's U.S. Patent 5,850,481 notes that the surface of a paper or other physical object can be textured with a pattern of micro-indentations to steganographically encode plural-bit information. The texturing is optically discernible, e.g., by a scanner, permitting the digital data to be decoded from scan data corresponding to the paper object.

In application 09/127,502, the present assignee taught various other arrangements by which blank media can be processed to encode a digital watermark. Some techniques employ very subtle printing, e.g.,

of fine lines or dots, which has the effect slightly tinting the media (e.g., a white media can be given a lightish-green cast). To the human observer the tinting appears uniform. Computer analysis of scan data from the media, however, reveals slight localized changes, permitting the multi-bit watermark payload to be discerned. Such printing can be by ink jet, dry offset, wet offset, xerography, etc.

Other techniques disclosed in the '502 application extend the texturing techniques first set forth in the '481 patent, e.g., by employing an intaglio press to texture the media as part of the printing process (either without ink, or with clear ink).

In accordance with certain embodiments of the present invention, machine-readable indicia (e.g., watermarks) are printed on, or in, media using inks having infrared or ultraviolet spectral characteristics, facilitating machine detection without compromising human invisibility. Still other embodiments employ inks that are chosen with regard to spectral illumination that may be expected from CRT displays in whose presence certain indicia may be sensed. A great many other embodiments and features are also disclosed.

Brief Description of the Drawings

Fig. 1 shows the spectral emission from a representative color computer monitor.

Detailed Description

In accordance with certain embodiments of the present invention, machine readable indicia can be printed on or in media (e.g., security documents, identification documents, etc.) using inks having infrared or ultraviolet spectral characteristics. A watermark printed with infrared-responsive ink, for example, may be sensed by many CCD detectors. (The spectral responses of many conventional CCD detectors extend somewhat into the infrared spectrum; the response at other wavelengths can be reduced by employing a suitable IR-passing filter layer between the CCD and object.) To the extent the ink's reflectance spectrum extends beyond the range viewable by humans, correspondingly more watermark energy may be encoded into the medium without regard to potentially objectionable human visible artifacts. Inks that are essentially transparent to visible light (i.e., essentially not visible) can be used to print machine-readable indicia on substrates without regard to subtleness or clever hiding tricks. They can form blatant patterns in the IR or UV spectrum, obviating the need for difficult signal-processing tricks to extract a weak data signal from a large noise signal. Watermark patterning, such as described below (e.g., binary checkerboards), can be used. So too with bar codes and other machine readable patterns.

The ink can be applied by any technique, including inkjet printing, wet-or dry-offfset, gravure, intaglio, etc. Moreover, the ink can be applied inside the media, or outside. In the former case, the media is formed in a process that introduces that permits marking of an interior portion. One such method is opacification of a translucent polymer film with several layers of ink or the like. Another is laminate construction. Such techniques, and the use of watermarking therein, are more particularly detailed in the application filed herewith entitled Digital Watermarking of Physical Objects, cited above

Marking outside the medium can be accomplished before other printing (e.g., while blank), as part of a printing process (e.g., intaglio application of inked line art to a banknote), or as an overprint after the visible printing design is formed. Such marking may be coextensive with the media, or may be limited to certain portions (e.g., areas that are otherwise blank, or – in an identity document – the bearer's photograph, etc.).

In accordance with another embodiment, each cash receptacle in a cash register drawer or the like is equipped with a small IR illumination source (e.g., LED), together with a 1-D or 2D sensor having sensitivity extending into the IR. The sensor, together with associated control and processor circuitry, can image and analyze a pattern taken from the top banknote placed in the receptacle to confirm that the detected pattern corresponds to that of an authentic banknote. A counterfeit note, produced e.g., with a conventional ink jet printer, will not have the telltale IR patterning, and can be flagged as illegitimate.

Such a sensor apparatus may also be fashioned as a stand-alone station for use at point of sale stations. Using such an apparatus, a cashier can check banknotes received from customers to confirm their authenticity.

A similar such device may "read" the denomination of a banknote from a watermark sensed by such a point-of-sale station or cash drawer. Any return change to be provided to the consumer can be calculated by an electronic terminal, without human data entry or opportunity for error.

Magnetic inks can likewise be used to boost machine detectability, providing a digital watermark signal that is less humanly-sensible than ordinary inks.

Two inks can be fashioned to have the same appearance to humans, but one have a spectrum that extends outside the visible spectrum (e.g., IR or UV). A substrate may be printed with one or more patterns that are printed partially with one ink and partially with the other. When sensed at IR or UV, parts of the pattern(s) disappear. Again, the inability of commonly available printing systems to print with such specialized inks provides a barrier to effective counterfeiting.

In applications 09/234,780 and 09/433,104, the present assignee disclosed systems in which two watermarks of different character are embedded in an object. The watermarks are designed to degrade differently in the presence of corruption, distortion, etc. In some embodiments, a "frailer" of the two watermarks may disappear when the encoded object undergoes any lossy manipulation.

Such an arrangement can similarly be effected by encoding two watermarks in a printed object, one of which watermarks is printed with an ink having characteristics not readily mimicable by conventional color printers (i.e., those based on cyan, magenta, yellow, and black colors). UV or IR spectral response is one such characteristic. Magnetic ink is another. A reproduction made with a conventional color printer will be missing one of the two watermarks, permitting an original to be distinguished from a copy.

Still other substrate markings can include combinations of visible and invisible (i.e., IR, UV, magnetic) markings.

In the present assignee's MediaBridge technology (detailed in applications 09/547,664, filed April 12, 2000, and), watermarked objects (e.g., magazine ads) held in front of an optical sensor (e.g., a camera) cause a coupled computer to link to an internet site associated with a code watermarked into the object. Many such cameras are adapted for mounting on top of, or near, a user's CRT monitor. The object held in front of the sensor may thus be illuminated – in whole or in part – by radiation from the phosphors of the CRT screen. Such phosphors have well defined spectral emissions (Fig. 1 is exemplary for monitors employing sulphide phosphors), and can serve as powerful illumination sources within certain spectral bands. According to yet another aspect of the present invention, the spectral radiation from a CRT is quantified, and the ink used to watermark an object is selected in accordance with such spectrum. Thus, for example, if a CRT produces a local maxima of spectral energy at a wavelength of 525 nanometers, and a local minima at 500 nanometers, use of an ink that reflects light of 525 nanometers would be advantageous. In contrast, if the ink reflects light at 500 nanometers, such effect would contribute little to watermark detectability but would instead serve only to make the watermark more visible to human observers. By using inks optimized to respond to the particular illumination expected from a monitor (or other predictable illumination source), machine detection of a watermark may be increased without increasing (but rather more generally decreasing) human visibility of the mark.

The same principles are equally applicable with other machine readable indicia – not just watermarks, but also bar codes, data glyphs, etc.

Since most color CRTs employ three color phosphors, a great variety of optimizations are possible.

One optimization is to drive the CRT with video signals causing the encoded object to be illuminated with light of known character. For example, the video driver signals may flash a frame of solid-red illumination (or just the red component of the frame otherwise being displayed) at a known instant of its operation. A watermark detection circuit, coupled to the video circuitry or triggered through a common control system, can sample an object presented before the CRT at that instant and have a priori knowledge of the light spectrum illuminating the object. In some embodiments, the optical sensor may be a narrow-band sensor (e.g., including an optical filter) and thus be sensitive only, e.g., to red illumination. By such arrangement, higher signal to noise ratios may be achieved in decoding, with less chance of false decoding.

In accordance with still another embodiment of the present invention, a 1- or 2-D a barcode is encoded with a watermark. The watermark may be formed of UV, IR, or magnetic ink, as detailed above. But it may also be formed of the same ink as the barcode. It is possible to apply the watermark to a barcode such that the barcode is still readable, yet became a carrier for the watermark. Such a watermark may be applied by overprinting the barcode with speckles of ink, slightly changing the local contrast. Or the markings (e.g., lines) comprising the barcode can be slightly changed – in position or width – to effect

the necessary luminance pattern of a desired watermark. (The slight changing of line placement or width to encode a watermark is more particularly detailed in application 09/074,034.)

The encoding of a barcode with a watermark can serve various purposes. One is as a hash code to confirm the validity of the barcode. Or the watermark may convey the same information as the barcode. Or the watermark may encode, or correspond in a predetermined manner, with other information on the object so-marked. (For example, in an identity document, the watermark may encode the bearer's name, or the document serial number. Or a hash of the serial number. Etc. Such arrangements are further discussed in patent 5,841,886.)

In some identity document (e.g., passport) embodiments, by either texturing, or adding holographic like features to a laminate, the laminate itself can become the carrier for the watermark. This can be with visible, retro-reflective, or UV/IR structures. Since document readers are able to process these covert features, images of the marked area would be available to the document inspector while being more obscured from the document holder (and potential forger / counterfeiter). (Laminate-marking and UV/IR technology is further discussed in the patents and applications cited above.)

According to yet another embodiment of the present application, a ghost image can be constructed, using line structures or special raster patterns, to reproduce a photo in an identity document. Such structure typically appears next to the bearer's photo in an identity document and serves as a potential carrier of a digital watermark. One benefit to this arrangement is that it is a personalized structure, so it is created as part of the document personalization process -- a perfect time to add a watermark. A watermark can also be encoded in a latent image that is designed to appear only under certain lighting or sampling conditions.

According to still another embodiment of the present invention, an object (either a physical object or a data object, such as audio, image, video) is encoded with multiple watermarks. One identifies a master document series / source or printing, and another identifies a subgroup (e.g., a particular person or group of objects). These two markings can work together or separately to enhance authentication and owner verification.

Still other embodiments comprise plastic card-based identity documents. A digital watermark can be applied to the front or the back, and to the plastic card "substrate" or to a photo.

A great variety of substrate marking techniques are known in the present assignee's patents and applications identified below. These techniques are likewise useful in connection with identity documents.

In the foregoing embodiments, the watermark signal can be represented as a checkerboard pattern comprising, e.g., a 96 x 96 array of elements, where each element is 0.012 inch on a side. Each component element can be light or dark, or intermediate grey-scale values may be used to further reduce visibility. Such checkerboards may be tiled together to span the full width and length of the media.

Alternatively, patterns other than checkerboards can be used. Such patterns (e.g., weave-like patterns), and methods for their generation, are detailed in the '005 and '502 applications cited above.

In most embodiments, the watermark payload is uniform across the medium. In some applications, however, it may be desirable to encode different payloads in different regions of a medium.

In other arrangements, the same watermark may be encoded in different places (e.g., on different sheets of media), but not by using the same pattern. Instead, different patterns can be used in different places to encode the same watermark payload.

The watermark can convey a payload of arbitrary length, commonly in the 2-256 bit range, perhaps most commonly between 24 and 72 bits. Error correcting coding, such as convolutional coding or BCH coding, can be employed to transform the base payload (e.g., 50 bits) to a longer data string (e.g., 96 – 1024 bits), assuring robustness in detection notwithstanding some data corruption (e.g., due to wear and tear of the medium, artifacts from scanning, etc.). The bits of this longer string are mapped, e.g., pseudo-randomly, to define the pattern (e.g., checkerboard).

An illustrative watermark-encoding technique is more particularly detailed in application 09/503,881, cited above (but is used without gain control and perceptual analysis since no image is present on the blank medium).

While the watermarking technique detailed in the just-cited application is preferred by the present assignee, it should be understood that the principles of the present invention can be employed with essentially any other watermarking technology. A great variety of such techniques are known.

Moreover, the invention finds application beyond "watermarking." Any form of machine-readable indicia, including 1- and 2-D barcodes and data glyphs, may be formed as noted above, and serve to facilitate machine-recognition of the media.

To provide a comprehensive disclosure without unduly lengthening this specification, the above-detailed patents and applications are incorporated herein by reference.

Having described and illustrated the principles of our invention with reference to specific embodiments, it will be recognized that the principles thereof can be implemented in other, different, forms.

For example, while one of the detailed embodiments contemplated changing the illumination provided by a monitor to optimize data detection, a filter can likewise be applied over the detector to eliminate wavelengths of unwanted light. In some sophisticated embodiments, the filtering can be electronically controlled, e.g., through use of known twisted nematic and other light shutter/filter technology.

The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

WE CLAIM:

1. A method of encoding an object with a machine readable marking encoding plural bits of binary data, characterized in that the method includes printing with an ink having an ultraviolet or infrared response, illuminating said printing with a light spectrum including ultraviolet or infrared energy, and sensing the printing using a sensor responsive to such ultraviolet or infrared energy.

2. The method of claim 1 that includes printing with an ink having an ultraviolet response, illuminating said printing with a light spectrum including ultraviolet energy, and sensing the printing using a sensor responsive to such ultraviolet energy.

3. The method of claim 1 that includes printing with an ink having an infrared response, illuminating said printing with a light spectrum including infrared energy, and sensing the printing using a sensor responsive to such infrared energy.

4. The method of claim 1 in which the machine readable indicia comprises a digital watermark.

5. The method of claim 1 in which the machine readable indicia comprises a bar code.

6. A method of sensing a watermark on a physical object, comprising illuminating the object with light emitted from a computer monitor, and controlling the computer monitor to change the light emitted therefrom so as to enhance detection of the watermark from the object.

7. A method of marking a medium with a machine readable indicia that encodes plural binary bits, the method including printing a first portion of said indicia using a first technique, and printing a second portion of said indicia using a second technique, said two portions appearing indistinguishably-printed to a human viewer thereof, but having characteristics facilitating their distinction by machine analysis.

8. The method of claim 7 in which the first technique employs a first ink, and the second technique employs a second ink, the first and second inks having differing spectral characteristics in the UV or IR spectrums.

9. A method of encoding a medium comprising forming a barcode on the medium, and digitally watermarking the barcode.

10. The method of claim 9 which includes overprinting barcode and digital watermark patterns.

11. The method of claim 9 that includes slightly altering the lines comprising the barcode to define thereby a digital watermark.

12. The method of claim 9 in which the barcode and the watermark each convey a plural-bit payload, and one payload serves as a check against the other.

13. A device for sensing a digital watermark from an object comprising:

a sensor; and

a filter interposed between the sensor and the object, the filter attenuating light in the visible spectrum, while substantially passing light in an IR or UV spectrum.

METHODS AND SYSTEMS FOR DIGITAL WATERMARKING

Abstract of the Disclosure

A variety of improvements to digital watermarking systems are disclosed, including use of UV and IR inks and illuminations, operation of computer monitors to tailor the illumination by which a machine-readable indicia is detected, anti-counterfeiting improvements to identification documents (e.g., passports), complementary use of barcodes and watermarks, etc.

APPENDIX F

DIGITAL WATERMARKING OF PHYSICAL OBJECTS

Related Application Data

The present application is a continuation-in-part of copending application 09/127,502, filed July 31, 1998.

The present application is related to copending applications 09/127,502, filed July 31, 1998; 09/437,357, filed November 10, 1999; 09/074,034, filed May 6, 1998; 09/234,780, filed 1/20/99; 09/433,104, filed November 3, 1999; 09/503,881, filed February 14, 2000; and application _____, filed April 20, 2000, entitled Image Patterns that Constitute Digital Watermarks.

The present application is also related to applications entitled Methods and Systems for Digital Watermarking, and Digital Watermarking Systems, both filed herewith.

The present application is also related to the assignee's patents 5,862,260, 5,850,481and 5,841,886.

Field of the Invention

The present invention relates to processing of physical media (e.g., blank printing stock, product packaging, catalogs, advertisements, etc.) to impart a machine-readable indicia (e.g., a plural-bit digital watermark) thereto.

Background and Summary of the Invention

Digital watermarking technology, a form of steganography, encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration.

Most commonly, digital watermarking is applied to digital objects, such as digital image, video, and audio. In the case of images, slight changes can be made to local luminance or color values to effect the encoding. These changes can later be detected by a computer, and analyzed to discern the watermark information represented thereby.

Digital watermarking techniques can also be applied to traditional physical objects, including blank paper. Such blank media, however, presents certain challenges since there is no image that can serve as the carrier for the watermark signal.

The assignee's U.S. Patent 5,850,481 notes that the surface of a paper or other physical object can be textured with a pattern of micro-indentations to steganographically encode plural-bit information. The texturing is optically discernible, e.g., by a scanner, permitting the (digital data to be decoded from scan data corresponding to the paper object.

In application 09/127,502, the present assignee taught various other arrangements by which blank media can be processed to encode a digital watermark. Some techniques employ very subtle printing, e.g., of fine lines or dots, which has the effect slightly tinting the media (e.g., a white media can be given a lightish-green cast). To the human observer the tinting appears uniform. Computer analysis of scan data from the media, however, reveals slight localized changes, permitting the multi-bit watermark payload to be discerned. Such printing can be by ink jet, dry offset, wet offset, xerography, etc.

Other techniques disclosed in the '502 application extend the texturing techniques first set forth in the '481 patent, e.g., by employing an intaglio press to texture the media as part of the printing process (either without ink, or with clear ink).

In one aspect, the present specification further develops and extends the techniques disclosed in the '502 application.

For example, printable media – especially for security documents (e.g., banknotes) and identity documents (e.g., passports) - is increasingly fashioned from synthetic materials. Polymeric films, such as are available from UCB Films, PLC of Belgium, are one example. Such films may be clear and require opacification prior to use as substrates for security documents. The opacification can be effected by applying plural layers of ink or other material, e.g., by gravure or offet printing processes. (Suitable inks are available, e.g., from Sicpa Securink Corp. of Springfield, VA.) In addition to obscuring the transparency of the film, the inks applied through the printing process form a layer that is well suited to fine-line printing by traditional intaglio methods. Such an arrangement is more particularly detailed in laid-open PCT publication WO98/33758. That application is believed to have a pending US counterpart application, which claims priority to Australian application 4847, filed January 29, 1997.

In accordance with certain embodiments of the present invention, a machine readable indicia encoding plural bits (e.g., a digital watermark) is embedded as part of such an opacification process.

Other security documents employ plural substrates bound together in a laminate structure. The laminates variously include paper, polypropylene film, polyethelyne film, polyurethane film, metal film, inks, adhesives, optically-variable devices (e.g., holograms), and other materials. (See, e.g., patents 5,935,696 and 5,618,630.) Again, in accordance with embodiments of the present invention, plural-bit machine readable indicia can be incorporated in such structures.

The foregoing and additional features and advantages of the invention will be more readily apparent from the following detailed description.

Detailed Description

As noted, one technique for forming a blank medium suitable for use as a security document is to gravure-print, or otherwise apply, plural layers of material (e.g., ink) to a synthetic substrate. In addition to making the substrate opaque (if it was not already), the layers provide a surface well suited for fine line offset or intaglio printing.

In known techniques, the layers added to the substrate are substantially uniform. In the case of gravure-printing of ink, the gravure printing plates are generally formed with a pattern of grooves designed to apply a substantially uniform layer of ink across the substrate.

In accordance with one embodiment of the present invention, one or more of the layers is non-uniform, and instead exhibits localized changes in ink density or tone (e.g., color) to effect a pattern in the resulting medium that is optically detectable from the finished substrate.

For gravure opacification, the changes in ink density can be effected by maintaining the same groove patterns as are utilized to effect uniform inking, but changing the groove size on a localized basis to deposit more ink at some locations, less at others. Alternatively, the changes in ink density can be effected by changing the groove patterns, e.g., to move adjoining lines closer together or farther apart, again with the aim of depositing ink more densely in some regions than others. Related techniques, albeit in a somewhat different context, are detailed in the '034 application cited above, and can be employed here.

Another technique of forming a pattern in one or more opacification layers is to use to laser to ablate portions of the layer, selectively removing material to form the desired pattern. Again, such a process results in a change visibly detectable from the exterior of the medium. (Laser ablation of an opacification layer is known in other contexts; see, e.g., laid-open PCT application WO9836913.)

In one embodiment, the watermark pattern is effected in only a single of the layers formed on the film substrate. In another embodiment, the pattern is effected in two or more of the layers. (The former approach avoids problem of plate-registration that arise in the latter. The latter may provide a marking that is more durable in the presence of wear than the former.) In still other embodiments, one layer may represent a first set of watermark data, and another may represent a second set of watermark data.

In another form of the invention, a security document medium is prepared in laminate fashion, with one or more of the interior layers formed so as to impart an optically-discernible pattern of contrast discernible from the exterior of the medium. The layer can be printed to form this pattern, or can be shaped to give such a result. The latter approach can employ a swiss cheese-like layer (formed, e.g., by laser cutting), where the holes in the layer give rise to an optical contrast effect from the exterior of the substrate that encodes the plural-bit data payload. The degree of contrast depends on the color of the layer, and the translucency of the exterior layer(s).

In some such embodiments an internal layer is paper, and exterior layers are synthetic. In others, an opposite arrangement is employed.

In the foregoing embodiments, or in embodiments in which a watermark signal is applied by printing to a finished substrate, the watermark can be deposited by ink jet printing or other dithered-technique, where the dither pattern is tailored to effect a luminance profile across a region that encodes a watermark.

The watermarking arrangement detailed in the '005 application can be employed both to the outside of a substrate as well as to a non-exterior component layer (whether laminate or opacification).

The algorithm employed in the '005 application can be altered, if desired, to provide a control by which a user can establish the degree of randomness to be included in the traversed path as the line(s) extend from one point to another. Likewise, a control can be provided to change a modulation effect (e.g., sinusoidal) applied to the direction or width of the line as it traverses a region.

It can be advantageous to apply various digital watermarking techniques to security badges and identity cards – of the sort commonly worn by employees at industrial facilities. Such cards are commonly printed by dedicated print stations that include both a personal computer and a specialized card printer. Datacard is one vendor of such systems. Information can be embedded on such cards (or in a non-surface layer and yet still sensible from the card exterior) in watermark form, embodying various data, e.g., the date of issuance, the owner name, an identification number, etc. The information can have the appearance of a tint or wash, as noted above, yet permit ready recovery of the embedded information.

In the foregoing embodiments, the watermark signal can be represented as a checkerboard pattern comprising, e.g., a 96 x 96 array of elements, where each element is 0.012 inch on a side. Each component element can be light or dark, or intermediate grey-scale values may be used to further reduce visibility. Such checkerboards may be tiled together to span the full width and length of the media.

Alternatively, patterns other than checkerboards can be used. Such patterns (e.g., weave-like patterns), and methods for their generation, are detailed in the '005 and '502 applications cited above.

In most embodiments, the watermark payload is uniform across the medium. In some applications, however, it may be desirable to encode different payloads in different regions of a medium. Such may be the case, for example, in pre-encoding blank pages for magazine stock. Each sheet (ultimately defining two magazine pages on its front and two on its back) may be arranged in columnar form (e.g., 3 columns per page), with each column bearing a different watermark. Still more complex arrangements, e.g., segregating each column into top, middle, and bottom thirds, can of course be used.

In other arrangements, the same watermark may be encoded in different places (e.g., on different sheets of media), but not by using the same pattern. Instead, different patterns can be used in different places to encode the same watermark payload.

The watermark can convey a payload of arbitrary length, commonly in the 2-256 bit range, and perhaps most commonly between 24 and 72 bits. Error correcting coding, such as convolutional coding or BCH coding, can be employed to transform the base payload (e.g., 50 bits) to a longer data string (e.g., 96 - 1024 bits), assuring robustness in detection notwithstanding some data corruption (e.g., due to wear and tear of the medium, artifacts from scanning, etc.). The bits of this longer string are mapped, e.g., pseudo-randomly, to define the pattern (e.g., checkerboard).

An illustrative watermark-encoding technique is more particularly detailed in application 09/503,881 (but is used without gain control and perceptual analysis since no image is present on the blank medium). The calibration signal there-detailed can be employed to permit decoding notwithstanding rotation or certain other corruptions of the detected watermark data.

While the watermarking technique detailed in the just-cited application is preferred by the present assignee, it should be understood that the principles of the present invention can be employed with essentially any other watermarking technology. A great variety of such techniques are known.

Moreover, the invention finds application beyond "watermarking." Any form of machine-readable indicia, including 1- and 2-D barcodes and data glyphs, may be formed as noted above, and serve to facilitate machine-recognition of the media.

To provide a comprehensive disclosure without unduly lengthening this specification, the above-detailed patents and applications are incorporated herein by reference.

The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

WE CLAIM:

1. In a method of forming a printable substrate that includes applying plural layers to a film substrate, an improvement comprising tailoring the tone or density of at least one of said layers to form a machine readable indicia encoding plural bits of digital data.

2. The method of claim 1 in which the indicia comprises a steganographic digital watermark pattern.

3. The method of claim 1 in which the film substrate is translucent, and the layers are opacification layers.

4. The method of claim 1 comprising tailoring the tone or density of at least one internal layer to form said indicia.

5. The method of claim 4 in which the tailoring comprises applying ink to an internal layer by an inkjet printing process.

6. The method of claim 1 in which the tailoring comprises applying ink with a gravure printing plate having grooves of non-uniform thickness formed therein.

7. The method of claim 1 in which the tailoring comprises applying ink with a gravure printing plate having non-uniformly distributed grooves formed therein.

8. The method of claim 1 in which the machine readable indicia is coextensive with the substrate.

9. A printable substrate formed according to the method of claim 1.

10. A banknote printed on the substrate of claim 9.

11. A printable substrate comprising a laminate structure including at least one internal layer, characterized in that said internal layer is formed with a machine readable indicia encoding plural binary bits, said indicia being optically detectable from outside said substrate.

12. The substrate of claim 11 in which the machine readable indicia is a digital watermark pattern.

13. The substrate of claim 11 in which the machine readable indicia is coextensive with the substrate.

14. The substrate of claim 11 in which at least one internal layer is formed of paper.

15. The substrate of claim 11 in which at least one internal layer is formed of a polymer.

16. The substrate of claim 11 in which at least one external layer is formed of paper.

17. The substrate of claim 11 in which at least one external layer is formed of a polymer.

18. The substrate of claim 11 in which the internal layer has gaps defined therein.

19. The substrate of claim 11 in which the internal layer is printed by an inkjet printing process.

20. The substrate of claim 11 in which the indicia encodes a calibration signal.

DIGITAL WATERMARKING OF PHYSICAL OBJECTS

Abstract of the Disclosure

A machine readable indicia is formed in a blank printable medium. The indicia may be formed in an opacification layer applied to a translucent substrate, or may be formed in a laminate layer. The indicia is optically detectable from the exterior of the medium, even if the indicia is not formed on the medium's exterior surface. One particular indicia is a seemingly-random weave-like pattern of lines defined in response to (1) a first user control that determines a degree of randomness of the line(s), (2) a second user control that determines a modulation effect to be applied to the line(s), and (3) the bits to be represented thereby. Many other indicia, including checkerboards, barcodes, data glyphs, etc., can also be used.

APPENDIX G

METHODS AND SYSTEMS FOR CONTROLLING COMPUTERS OR LINKING TO INTERNET RESOURCES FROM PHYSICAL AND ELECTRONIC OBJECTS

Related Application Data

This application claims priority to each of the following copending applications:

?? *09/314,648, filed 5/19/99*
?? *09/342,688, filed 6/29/99*
?? *09/342,689, filed 6/29/99*
?? *09/342,971, filed 6/29/99*
?? *09/343,101, filed 6/29/99*
?? *09/343,104, filed 6/29/99*
?? *60/141,468, filed 6/29/99*
?? *60/151,586, filed 8/30/99*
?? *60/158,015, filed 10/6/99*
?? *60/163,332, filed 11/3/99*
?? *60/164,619, filed 11/10/99*
?? *09/531,076, filed 3/18/00*
?? *09/543,125, filed 4/6/00*
?? *09/547,664, filed 4/12/00*
?? *09/552,998, filed 4/13/00*

Background and Summary of the Invention

"Bedoop." That might be the sound someone might hear as they lazily place a magazine advertisement in front of their desktop camera. Magically, the marketing and sales web site associated with the ad is displayed on their computer. More information? Want to buy now? Look at the full product line? No problem.

"Bedoop." That might be the same sound when that same someone places their credit card in front of their desktop camera. Instantly, the product displayed on the web page is purchased. Behind the scenes, a secure purchase link is initiated, transmitting all requisite information to the vendor. Twist the credit card clockwise and the purchaser chooses overnight delivery.

So goes an exemplary embodiment further described in this specification. Although this example is rather specific, it nevertheless alludes to vast array of applications possible when an input device such as a digital camera is turned into a general-purpose user interface device with an intuitive power that very well might rival the mouse and the keyboard.

One aspect of certain embodiments is that an object or paper product so-scanned contains digital information that can be quickly read and acted upon by an appropriately configured device, computer or appliance. Such an embodiment envisions that this digital information is aesthetically hidden on objects. These objects have been previously and pro-actively marked with the digital information, using any of the broad range of data encoding technologies, such as digital watermarking.

Although this aspect of the technology concentrates on flat object applications wherein the digital information is often imperceptibly integrated into the object, it is certainly not meant to be so limited. Objects can be three dimensional in nature and the information more visually overt and/or pre-existing (i.e., not "pro-actively" embedded, or it might not even be "digital," per se). Different implementation considerations attach to these variants. Likewise, though the bulk of this disclosure concentrates on objects which have some form of digital message attached thereto, some aspects of the technology may apply to objects which have no such thing, where the prior arts of pattern recognition and gestural input can be borrowed in combination with this technology to effect yet a broader array of applications.

Nor, as will be apparent, is the technology limited to systems employing optical input and encoded imagery. Corresponding techniques can also be employed with encoded audio. Indeed, any physical or electronic "object" can make use of the principles detailed herein.

"Bedoop." The sound that a refrigerator might make, outfitted with a simple camera/ processor unit/net connection, as a ten year old child holds up an empty milk carton and a ping goes out to the local grocery store, adding the item to an accumulating delivery list. The sound that might be heard echoing over and over inside Internet cafés as heretofore computerphobes take their first skeptical steps onto the World Wide Web. The sound heard at the fast food counter as a repeat customer holds up his sandwich card ticking off his latest meal, hoping for the sirens to go off for a $500 prize given to the lucky customer of the week. Blue sky scenarios abound.

Such aspects of the present technology are thus about powerful new user interfaces to computers. These new user interfaces extend into the everyday world in ways that a mouse and keyboard never could. By enabling everyday objects to communicate their identities and functions to ever-attendant devices, not only will the World Wide Web be given an entirely new dimension, but basic home and office computing may be in store for some fundamental advances as well.

According to one aspect, the invention includes a method of data processing on a computer system, comprising (a) using an application program to compose an electronic version of a document; (b) printing the document onto paper, the printing including marking with machine readable indicia encoding plural-bit auxiliary data; and (c) storing the plural-bit auxiliary data in association with data identifying a location at which the electronic version of the document is stored.

According to another aspect, the invention includes a method of data processing on a computer system, comprising (a) presenting a printed document to an optical capture device; (b) processing image data produced by said device to decode plural-bit data encoded therein; (c) based on said decoded plural-bit data, launching a software application corresponding to said printed document; and (d) using said software application to open an electronic version of said document.

According to another aspect, the invention includes a method of operating a computer, the computer including an operating system with a registry database, the registry database associating specific data types with specific software programs particularly corresponding thereto, wherein the method further

includes: (a) providing a frame of image data; (b) decoding plural-bit identifier data from the image data; (c) consulting the registry database to identify a software program corresponding to said identifier data; and (d) invoking the identified software program.

According to another aspect, the invention includes a greeting card having a substrate with visually-perceptible indicia printed thereon, wherein the card is encoded with plural-bit binary data that can be decoded by an image processing device and used to direct a computer to a web site where an image, video, and/or audio presentation corresponding to said card is provided.

According to another aspect, the invention includes a method of providing a customized greeting, comprising: (a) providing a greeting card having plural-bit data encoded therein; (b) customizing a web site presentation corresponding to said card; (c) providing the card to a recipient; (d) decoding the encoded plural-bit data from the card; and (e) in response to the decoded plural-bit data, presenting to the recipient the web site presentation.

According to another aspect, the invention includes a method of printing a magazine, comprising: (a) processing an electronic representation of an advertisement to encode plural bit data therein; (b) printing a page of advertising in accordance with said electronic representation to yield an encoded advertisement page; and (c) binding said page into a magazine; wherein said plural bit data serves to identify an entry in a database, said database entry having an internet address of a web page that is associated with said advertisement stored therein.

According to another aspect, the invention includes a promotional method comprising: (a) encoding a print advertisement to hide plural-bit data therein; (b) processing the print advertisement to extract the plural-bit data therefrom; and (c) using at least a part of the extracted plural-bit data to direct an internet web browser to a web site that provides consumer information related to a product or service promoted by the print advertisement.

According to another aspect, the invention includes a method of determining consumer response to print advertising, comprising: (a) encoding a first print advertisement with first data; (b) encoding a second print advertisement with second data different than the first; (c) the first and second data providing identifiers by which consumer devices can link to web pages associated with said advertisements; (d) monitoring linking traffic due to each of said identifiers to thereby determine consumer response to the advertisements.

According to another aspect, the invention includes a promotional method comprising: (a) presenting an object within the field of view of an optical sensor device, the object being selected from the list consisting of a retail product, packaging for a retail product, or printed advertising; (b) acquiring optical data corresponding to the object; (c) decoding plural-bit digital data from the optical data; (d) submitting at least some of said decoded data to a remote computer; and (e) determining at the remote computer whether a prize should be awarded in response to submission of said decoded data.

According to another aspect, the invention includes a method of interacting with a magazine using a computer, the computer including an internet web browser, the method including: (a) providing a peripheral device having a sensor; (b) positioning the peripheral device adjacent a first advertisement in the magazine to direct the web browser to a first internet address; and (c) positioning the peripheral device adjacent a second advertisement in the magazine to direct the web browser to a second internet address.

According to another aspect, the invention includes a computer peripheral and method of its use, the peripheral being used in conjunction with a computer system having an internet browser associated therewith, the peripheral comprising: (a) a housing adapted to fit within a user's palm and slide over a medium; (b) an optical sensor having at least one sensing element and producing optical data; (c) a lens for imaging the medium onto the sensor; and the method includes: (a) sliding the peripheral over a portion of a printed advertisement; (b) processing the optical data to decode plural bit information encoded on the advertisement; and (c) using said plural bit information to direct the internet browser to an internet web page associated with said advertisement.

According to another aspect, the invention includes an electronic commerce method comprising: (a) providing a printed catalog that includes an image of an article offered for sale by a merchant, wherein the image is encoded with plural-bit binary data; (b) optically sensing the image to produce optical data corresponding thereto; (c) decoding the encoded data from the optical data; and (d) electronically ordering the article from the merchant by use of said decoded data. The ordering may make use of earlier-stored customer profile information (e.g., clothing size data), and the encoding may be steganographic.

According to another aspect, the invention comprises a wireless telephony handset including a microphone, a modulator, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation, the handset further including an optical sensor producing optical data, a lens for imaging an object onto the sensor, and a decoder for decoding plural bit identifier data conveyed by a barcode or a digital watermark on the object.

According to another aspect, the invention includes an image-based network navigation method permitting a user to link to a remote computer, comprising: (a) detecting encoded data from a printed object; (b) linking to the remote computer through a network in accordance with said encoded data; and (c) providing the user's zip code to the remote computer.

According to another aspect, the invention includes a method comprising: (a) sensing an object identifier from a first object; (b) sending said first object identifier from a first device to a second device; (c) in response, at said second device, identifying address information corresponding to said first object identifier and sending same to the first device; (d) initiating a link from the first device in accordance with said address information; (e) at said second device, identifying additional objects related to said first object; identifying additional address information corresponding to said additional objects; and sending said additional address information to the first device; and (f) storing said additional address information in a memory at the first device; wherein, if an object included among said identified additional objects is

sensed by the first device, the corresponding address information can be retrieved from said memory in the first device without the intervening delays of communicating with the second device.

According to another aspect, the invention includes an apparatus having a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) an identifier of said software program, and (b) at least a portion of detected machine readable data.

According to another aspect, the invention includes an apparatus having a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) a context or environment identifier, and (b) at least a portion of detected machine readable data.

According to another aspect, the invention includes a networked computer system, responsive to watermark data sent from a software program on a remote computer, to initiate delivery of advertisement data to said remote computer.

In any of the foregoing arrangements, the encoding can be steganographic (e.g., by digital watermarking), or can employ other machine readable data (e.g., barcodes, etc.). More generally, the arrangements just reviewed generally have counterparts that can be implemented with other than optical or image data (e.g., audio data, magnetic stripe information, etc.).

The foregoing just touches on a few of the many inventive aspects of the technology detailed below. These and other features of the present technology will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a diagram showing the principal process components of an illustrative system employing the present technology.

Fig. 2 is a block diagram showing an illustrative system for performing the response process of Fig. 1.

Fig. 3 is a block diagram more particularly detailing an originating device used in the system of Fig. 2.

Fig. 4 illustrates certain top level data flows in the system of Fig. 2.

Fig. 5 illustrates certain data flows associated with the router of Fig. 2.

Fig. 6 illustrates certain data flows associated with the registration process of Fig. 2.

Fig. 7 illustrates certain data flows associated with the product handler of Fig. 2.

Figs. 8-10 show a sequence of screen shots from an illustrative system.

Fig. 11 is a block diagram showing another embodiment of the present technology.

Fig. 12 is a block diagram showing another embodiment of the present technology.

Fig. 13 is a block diagram of a prior art scanner.

Fig. 14 shows an object being scanned along an arced path.

Fig. 15 shows how object warping may be detected.

Fig. 16 shows use of binocular processing to determine certain object attributes.

Fig. 17 shows a watermark grid.

Fig. 18 shows a pre-warped watermark grid.

Fig. 19 shows another pre-warped watermark grid.

Detailed Description

Basically, the technology detailed in this disclosure may be regarded as enhanced systems by which users can interact with computer-based devices. Their simple nature, and adaptability for use with everyday objects (e.g., milk cartons), makes the disclosed technology well suited for countless applications.

Due to the great range and variety of subject matter detailed in this disclosure, an orderly presentation is difficult to achieve. For want of a better arrangement, the specification is broken into two main parts. The first part details a variety of methods, applications, and systems, to illustrate the diversity of the present technology. The second more particularly focuses on a print-to-internet application. A short concluding portion is presented in Part III.

As will be evident, many of the topical sections presented below are both founded on, and foundational to, other sections. For want of a better rationale, the sections in the first part are presented in a more or less random order. It should be recognized that both the general principles and the particular details from each section find application in other sections as well.

Compounding the situation, the present specification draws from several priority applications filed over the course of nearly a year. Accordingly, the same concepts are sometimes expressed several times, each reflecting a different perspective – depending on the date and context of the application in which it was first found.

The term "Bedoop" has been superceded in applicant's commercialization of the technology by the term Digimarc MediaBridge. Both terms are used in this specification but refer to the same technology.

To prevent the length of this disclosure from compounding out of control, the various permutations and combinations of the features of the different sections are not exhaustively detailed. The inventors intend to explicitly teach such combinations/permutations, but practicality requires that the detailed synthesis be left to those who ultimately implement systems in accordance with such teachings.

PART I

Introduction to Digital Watermarking and other Encoding Techniques

There are nearly as many techniques for digital watermarking (a type of steganographic data encoding) as there are applications for it. The reader is presumed to be familiar with the great variety of methods. A few are reviewed below.

The present assignee's prior application 09/127,502, filed July 31, 1998, now published as WO0007356, shows techniques by which very fine lines can be printed on a medium to slightly change the medium's apparent tint, while also conveying digital data. Commonly-owned application 09/074,034, filed May 6, 1998, now published as WO 9953428, details how the contours of printed imagery can be adjusted to convey digital data. (That technique can be applied to printed text characters, as well as the line art imagery particularly considered.) The assignee's patent 5,850,481 details how the surface of paper or other media can be textured to convey optically-detectable binary data. The assignee's patents 5,862,260, 5,841,886 and 5,809,160 detail various techniques for steganographically encoding photographs and other imagery.

Some watermarking techniques are based on changes made in the spatial domain; others are based on changes made in transformed domains (e.g., DCT, wavelet).

Watermarking of printed text can be achieved by slight variations to character shape, character kerning, line spacing, etc., as shown by various writings by Brassil et al, including "Electronic Marking and Identification Techniques to Discourage Document Copying," Proceedings of INFOCOM '94 Conference on Computer, IEEE Comm. Soc Conference, June 12-16, 1994, pp. 1278-1287; "Hiding Information in Document Images," Proceedings of the Twenty-Ninth Annual Conference on Information Sciences and Systems, p. 482-9, 1995; and "Document marking and identification using both line and word shifting," Proceedings of IEEE INFOCOM '95, The Conference on Computer Communications. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies; Bringing Information to People (Cat. No.95CH35759), p. 853-60 vol.2, 1995.

The foregoing is just a sampling of the large literature on watermarking. The artisan is presumed to be familiar with such art, all of which is generally suitable for use with the novel concepts detailed below.

Although the following specification focuses on applications employing digital watermarking, certain of such applications can alternatively employ other data encoding techniques, including 1D and 2D barcodes, magnetic ink character recognition (MICR), optical character recognition (OCR), optical mark recognition (OMR), radio frequency identification (RF/ID), UV/IR identification technologies, data glyphs, organic transistors, magnetic stripe, etc., depending on the particular application requirements.

Basic Principles – Refrigerators and Desktop Clutter

Referring to Fig. 11, a basic embodiment 110 of the present technology includes an optical sensor 112, a computer 114, and a network connection 116 to the internet 118. The illustrated optical sensor 112 is a digital camera having a resolution of 320 by 200 pixels (color or black and white) that stares out, grabbing frames of image data five times per second and storing same in one or more frame buffers. These frames of image data are analyzed by a computer 114 for the presence of Bedoop data. (Essentially, Bedoop data is any form of plural-bit data encoding recognized by the system 110 -- data which, in many

embodiments, initiates some action.) Once detected, the system responds in accordance with the detected Bedoop data (e.g., by initiating some local action, or by communication with a remote computer, such as over the internet, via an online service such as AOL, or using point-to-point dial-up communications, as with a bulletin board system).

Consider the milk carton example. The artwork on a milk carton can be adapted to convey Bedoop data. In the preferred embodiment, the Bedoop data is steganographically encoded (e.g., digitally watermarked) on the carton. Numerous digital watermarking techniques are known – all of which convey data in a hidden form (i.e., on human inspection, it is not apparent that digitally encoded data is present). Exemplary techniques operate by slightly changing the luminance, or contours of selected points on artwork or text printed on the carton, or by splattering tiny droplets of ink on the carton in a seemingly random pattern. Each of these techniques has the effect of changing the local luminance at areas across the carton – luminance changes that can be detected by the computer 114 and decoded to extract the encoded digital data. In the case of a milk carton, the data may serve to identify the object as, e.g., a half gallon carton of Alpenrose brand skim milk.

The Fig. 11 apparatus can be integrated into the door of a refrigerator and used to compile a shopping list. Milk cartons, and other Bedoop-encoded packaging, can be held up the optical sensor. When the computer 114 detects the presence of Bedoop data and successfully decodes same, it issues a confirmation tone ("be-doop") from a speaker or other audio transducer 122. The computer then adds data identifying the just-detected object to a grocery list. This list can be maintained locally (in disk storage or non-volatile RAM 124 or the like in the refrigerator or elsewhere in the home), or remotely (e.g., at a server computer located at a user-selected grocery, or elsewhere). In either event, the list is desirably displayed on a display in the user's home (e.g., an LCD screen 126 built into the front of the appliance). Conventional user interface techniques can be employed permitting the user to scroll through the displayed list, delete items as desired, etc.

Periodically, the listed groceries can be purchased and the list cleared. In one embodiment, the list is printed (either at the home or at the grocery), and the user walks the grocery aisles and purchases same in the conventional manner. In another embodiment, the grocer pulls the listed items from the shelves (in response to a user request conveyed by the internet or telephone, or by a gesture as hereafter detailed). Once the list has been pulled, the grocer can alert the user that the groceries are available for pickup (again, e.g., by internet or telephone message), or the grocer can simply deliver the groceries directly to the user's home. Naturally, on-line payment mechanisms can be employed if desired.

Consider a wholly unrelated Bedoop application. A Microsoft Excel spreadsheet is printed onto paper, and the paper becomes buried in a stack of clutter on an office worker's desk. Months later the spreadsheet again becomes relevant and is dug out of the stack. Changes need to be made to the data, but the file name has long-since been forgotten. The worker simply holds the printed page in front of a camera

associated with the desktop computer. A moment later, the electronic version of the file appears on the worker's computer display.

When the page was originally printed, tiny droplets of ink or toner were distributed across the paper in a pattern so light as to be essentially un-noticeable, but which steganographically encoded the page with a plural-bit binary number (e.g., 24-128 bits). A database (e.g., maintained by the operating system, the Excel program, the printer driver, etc.) stored part of this number (e.g., 20 bits, termed a Universal Identifier, or UID) in association with the path and file name at which the electronic version of the file was stored, the page number within the document, and other useful information (e.g., author of the file, creation date, etc.).

The steganographic encoding of the document, and the updating of the database, can be performed by the software application (e.g., Excel). This option can be selected once by the user and applied thereafter to all printed documents (e.g., by a user selection on an "Options" drop-down menu), or can be presented to the user as part of the Print dialog window and selected (or not) for each print job.

When such a printed page is later presented to the camera, the computer automatically detects the presence of the encoded data on the page, decodes same, consults the database to identify the file name/location/page corresponding to the 20-bit UID data, and opens the identified file to the correct page (e.g., after launching Excel). This application is one of many "paper as portal" applications of the Bedoop technology.

The foregoing are but two of myriad applications of the technology detailed herein. In the following discussion a great many other applications are disclosed. However, regardless of the length of the specification, it is possible only to begin to explore a few of the vast ramifications of this technology.

A few more details on the basic embodiments described above may be helpful before delving into other applications.

Optics

For any system to decode steganographically encoded data from an object, the image of the object must be adequately focused on the digital camera's CCD (or other, e.g., CMOS) sensor. In a low cost embodiment, the camera has a fixed nominal focal length, e.g., in the range of 2-24 inches (greater or lesser lengths can of course be used). Since the camera is continuously grabbing and analyzing frames of data, the user can move the object towards- or away- from the sensor until the decoder succeeds in decoding the steganographically encoded data and issues a confirming "Bedoop" audio signal.

In more elaborate embodiments, known auto-focusing technology can be employed.

In still other embodiments, the camera (or other sensor) can be equipped with one or more auxiliary fixed-focus lenses that can be selectively used, depending on the particular application. Some such embodiments have a first fixed focused lens that always overlies the sensor, with which one or more auxiliary lenses can be optically cascaded (e.g., by hinge or slide arrangements). Such arrangements are

desirable, e.g., when a camera is not a dedicated Bedoop sensor but also performs other imaging tasks. When the camera is to be used for Bedoop, the auxiliary lens is positioned (e.g., flipped into) place, changing the focal length of the first lens (which may by unsuitably long for Bedoop purposes, such as infinity) to an appropriate Bedoop imaging range (such as one foot).

Other lens-switching embodiments do not employ a fixed lens that always overlies the sensor, but instead employ two or more lenses that can be moved into place over the sensor. By selecting different lenses, focal lengths such as infinity, six feet, and one foot can be selected.

In all such arrangements, it is desirable (but not essential) that the steganographically-encoded portion of the object being imaged fills a substantial part of the image frame. The object can be of various sizes, e.g., a 10 by 12 inch front panel of a cereal box, or a proof of purchase certificate that is just one inch square. To meet this requirement, small objects need to be placed closer to the camera than large objects. The optics of the system can be designed, e.g., by selection of suitable aperture sizing and auxiliary lighting (if needed), to properly image objects of various sizes within a range of focal distances.

Some embodiments avoid issues of focal distances and identifying the intended object by constraining the size of the object and/or its placement. An example is a business card reader that is designed for the sole task of imaging business cards. Various such devices are known.

Decoding/Encoding

The analysis of the image data can be accomplished in various known ways. Presently, most steganographic decoding relies on general purpose microprocessors that are programmed by suitable software instructions to perform the necessary analysis. Other arrangements, such as using dedicated hardware, reprogrammable gate arrays, or other techniques, can of course be used.

The steganographic decoding process may entail three steps. In the first, the object is located. In the second, the object's orientation is discerned. In the third, the Bedoop data is extracted from the image data corresponding to the Bedoop object.

The first step, object location, can be assisted by various clues. One is the placement of the object; typically the center of the image field will be a point on the object. The surrounding data can then be analyzed to try and discern the object's boundaries.

Another location technique is slight movement. Although the user will typically try to hold the object still, there will usually be some jitter of the Bedoop object within the image frame (e.g., a few pixels back and forth). Background visual clutter, in contrast, will typically be stationary. Such movement may thus be sensed and used to identify the Bedoop object from within the image data.

Still another object-location clue is object shape. Many Bedoop objects are rectangular in shape (or trapezoidal as viewed by the camera). Straight edge boundaries can thus be used to define an area of likely Bedoop data.

Color is a further object identification clue that may be useful in some contexts.

Yet another object location clue is spatial frequency. In imaging systems with well defined focal zones, undesired visual clutter may be at focal distances that results in blurring. The Bedoop object, in contrast, will be in focus and may be characterized by fine detail. Analyzing the image data for the high frequencies associated with fine detail can be used to distinguish the intended object from others.

Characteristic markings on the object (as discussed below in connection with determining object orientation) can also be sensed and used in locating the object.

Once the Bedoop object has been located within the image data, masking can be applied (if desired) to eliminate image data not corresponding to the intended object.

The next step in the decoding process, determining orientation of the Bedoop data, can likewise be discerned by reference to visual clues. For example, some objects include subliminal graticule data, or other calibration data, steganographically encoded with the Bedoop data to aid in determining orientation. Others can employ overt markings, either placed for that sole purpose (e.g. reference lines or fiducials), or serving another purpose as well (e.g. lines of text), to discern orientation. Edge-detection algorithms can also be employed to deduce the orientation of the object by reference to its edges.

Some embodiments filter the image data at some point in the process to aid in ultimate Bedoop data extraction. One use of such filtering is to mitigate image data artifacts due to the particular optical sensor. For example, CCD arrays have regularly-spaced sensors that sample the optical image at uniformly spaced discrete points. This discrete sampling effects a transformation of the image data, leading to certain image artifacts. An appropriately configured filter can reduce some of these artifacts.

(In some arrangements, the step of determining the orientation can be omitted. Business card readers, for example, produce data that is reliably free of artifacts and is of known scale. Or the encoding of the Bedoop data can be effected in such a way that renders it relatively immune to certain distortion mechanisms. For example, while the presently-preferred encoding arrangement operates on a 2D grid basis, with rows and columns of data points, the encoding can alternatively be done on another basis (e.g., a rotationally-symmetric form of encoding, so that rotational state of the image data can be ignored). In still other embodiments, the orientation-determining step can be omitted because the decoding can readily proceed without this information. For example decoding which relies on the Fourier-Mellin transform produces data in which scale and rotation can be ignored.)

Once the orientation of the object is discerned, the image data may be virtually re-registered, effectively mapping it to another perspective (e.g., onto a rectilinear image plane). This mapping can employ known image processing techniques to compensate, e.g., for rotation state, scale state, differential scale state, and X-Y offset, of the original Bedoop image data. The resulting frame of data may then be more readily processed to extract the steganographically-encoded Bedoop data.

In an exemplary embodiment, after the image data is remapped into rectilinear planar form, subliminal graticule data is sensed that identifies the locations within the image data where the binary data is encoded. Desirably, the binary data is redundantly encoded, e.g., in blocks of eight-by-eight patches.

Each patch comprises one or more pixels. (The patches are typically square, and thus contain 1, 4, 9, or 16, etc. pixels.) The nominal luminance of each patch before encoding (e.g., artwork pre-existing on the object) is slightly increased or decreased to encode a binary "1" or "0." The change is slight enough to be generally imperceptible to human observers, yet statistically detectable from the image data – especially if several such blocks are available for analysis. Preferably, the degree of change is adapted to the character of the underlying image, with relatively greater changes being made in regions where the human eye is less likely to notice them. Each block thus encoded can convey plural bits of data (e.g., 16 – 128 bits). The encoding of such blocks in tiled fashion across the object permits the data to be conveyed in robust fashion.

Much of the time, of course, the Bedoop sensor is staring out and grabbing image frames that have no Bedoop data. Desirably, the detection process includes one or more checks to assure that Bedoop data is not wrongly discerned from non-Bedoop image data. Various techniques can be employed to validate the decoded data, e.g., error detecting codes can be included in the Bedoop payload and checked to confirm correspondence with the other Bedoop payload. Likewise, the system can confirm that the same Bedoop data is present in different tiled excerpts within the image data, etc.

Details of particular encoding and decoding techniques can be found in U.S. patent 5,862,260 and application 09/503,881, the disclosures of which are incorporated by reference. As noted, the data can be encoded on a tiled basis, with each tile being 64 to 256 elements on a side. Each element can be 0.01 inches square. The Bedoop payload data can be redundantly represented by various error-tolerant coding techniques (e.g., convolutions coding, trellis coding, turbo codes, etc.) to fill the tiled block. Each bit is thus redundantly encoded, with a "1" being represented as an increase at certain pixels, and as a decrease at other pixels. The increases and decreases can be scaled in accordance with visual masking attributes of the image being encoded. The calibration signal can be summed with the tiled data signal and can comprise a signal tailored in the frequency domain to have 12 – 64 spectral impulses per quadrant, in a known pattern. During detection, the rotation or scaling of these impulses from their known frequency domain coordinates permits the rotation or scaling of the image to be discerned and compensated for.

Data Structures, Formats, Protocols, and Infrastructures

In an exemplary system, the Bedoop data payload is 64 bits. This payload is divided into three fields CLASS (12 bits), DNS (24 bits) and UID (24 bits). (Other payload lengths, fields, and divisions, are of course possible, as is the provision of error-checking or error-correcting bits.)

Briefly, the CLASS ID is the most rudimentary division of Bedoop data, and may be analogized, in the familiar internet taxonomy, to the limited number of top level domains (e.g., .com, .net, .org, .mil, .edu, .jp, .de, .uk, etc.). It is basically an indicator of object type. The DNS ID is an intermediate level of data, and may be analogized to internet server addresses (e.g., biz.yahoo, interactive.wsj, etc.) The UID is the

finest level of granularity, and can roughly be analogized to internet pages on a particular server (e.g., edition/current/summaries/front.htm, daily/home/default.hts, etc.).

Generally speaking, the CLASS ID and DNS ID, collectively, indicate to the system what sort of Bedoop data is on the object. In the case of Bedoop systems that rely on remote servers, the CLASS and DNS IDs are used in identifying the server computer that will respond to the Bedoop data. The UID determines precisely what response should be provided.

In the case of a refrigerator Bedoop system, what happens if an object with an unfamiliar CLASS/DNS ID data is encountered? The system can be programmed not to respond at all, or to respond with a raspberry-like sound (or other feedback) indicating, "I see a Bedoop object but don't know what to do with it."

Most systems will be able to respond to several classes of Bedoop objects. Simple software-based systems can compare the CLASS/DNS ID (and optionally the UID) to fixed values, and can branch program execution to corresponding subroutines. Likewise, hardware-based systems can activate different circuitry depending on the detected CLASS/DNS ID.

In the case of a computer equipped with a Bedoop input device (e.g., a Sony VAIO PictureBook laptop with built-in camera, or a desktop personal computer with a tethered camera), the operating system's registry database can be employed to associate different application programs with different CLASS/DNS IDs (just as the .XLS and .DOC file extensions are commonly associated by existing operating system registries to invoke Microsoft Excel and Word software applications, respectively). When a new Bedoop application is installed, it logs an entry in the registry database indicating the CLASS/DNS ID(s) that it will handle. Thereafter, when an object with such a CLASS/DNS ID is encountered, the operating system automatically launches the corresponding application to service the Bedoop data in an appropriate manner.

Sometimes the computer system may encounter a Bedoop object for which it does not have a registered application program. In such case, a default Bedoop application can be invoked. This default application can, e.g., establish an internet link to a remote server computer (or a network of such computers), and can transmit the Bedoop data (or a part of the Bedoop data) to that remote computer. The remote server can undertake the response itself, it can instruct the originating computer how to respond appropriately, or it can undertake some combination of these two responses. (Such arrangements are further considered below.)

Fig. 12 shows an illustrative architecture employing the foregoing arrangement.

At a local Bedoop system 128 (which may be implemented, for example, using a conventional personal computer 129), a camera, scanner, or other optical sensor 130 provides image data to a decoder 132 (which may be implemented as a software component of the operating system 133). The decoder 132 analyzes the image data to discern the plural-bit Bedoop data. The CLASS ID of this Bedoop data is

applied to a Bedoop registry 134. The registry responds by identifying and launching a local Bedoop application 136 designed to service the discerned Bedoop data.

Sometimes the system 128 may encounter a Bedoop object for which several different responses may be appropriate. In the case of a printed office document, for example, one response may be as described above – to present the electronic version of the file on a computer, ready for editing. But other responses may also be desired, such as writing an email message to the author of the printed document, with the author's email address already specified in the message address field, etc.

Such different responses may be handled by different Bedoop applications, or may be options that are both provided by a single Bedoop application. In the former case, when the CLASS/DNS IDs are decoded and provided to the operating system, the registry indicates that there are two (or more) programs that might be invoked. The operating system can then present a dialog box to the user inviting the user to specify which form of response is desired. Optionally, a default choice can be made if the user doesn't specify within a brief period (e.g., three seconds). The operating system can then launch the Bedoop application corresponding to the chosen response.

A similar arrangement can be employed if a single Bedoop application can provide both responses. In such case the operating system launches the single Bedoop application (since there is no ambiguity to be resolved), and the application presents the choice to the user. Again, the user can select, or a default choice can be automatically made.

In the just-described situations, the user can effect the choice by using the keyboard or mouse – as with traditional dialog boxes. But Bedoop provides another, usually easier, form of interaction. The user can make the selection through the optical sensor input. For example, moving the object to the right can cause a UI button on the right side of the dialog box to be selected; moving the object to the left can cause a UI button on the left side of the dialog box to be selected; moving the object towards the camera can cause the selected button to be activated. Many other such techniques are possible, as discussed below.

If the registry 134 does not recognize, or otherwise does not know how to respond to Bedoop data of that particular CLASS/DNS, the registry launches a default Bedoop client application. This client application, in turn, directs a web browser 40 on the local Bedoop system 128 to communicate with a remote master registration server computer 42. The local computer forwards the Bedoop data to this master server. The master server 42 examines the CLASS ID, and forwards the Bedoop data (directly, or through intervening servers) to a corresponding CLASS server 44. (A single server may handle Bedoop data of several classes, but more typically there is a dedicated server for each CLASS.)

Each CLASS server 44 serves as the root of a tree 46 of distributed DNS servers. A DNS server 48a, for example, in a first tier 50 of the DNS server tree, may handle Bedoop data having DNS IDs beginning with "000." Likewise, DNS server 48b may handle Bedoop data having DNS IDs beginning with "001," etc., etc.

Each DNS server in the first tier 50 may, in turn, route Bedoop data to one of 8 servers in a second tier of the tree, in accordance with the fourth- through sixth bits of the DNS data. The tree continues in this fashion until a terminal level of DNS leaf node servers 56.

Ultimately, Bedoop data routed into this network reaches a DNS leaf node server 56. That leaf node server may handle the Bedoop data, or may redirect the local Bedoop system to a further server 58 that does so. That ultimate server – whether a DNS leaf node server or a further server – can query the local Bedoop system for further information, if necessary, and can either instruct the local Bedoop system how to respond, or can undertake some or all of the response itself and simply relay appropriate data back to the local Bedoop system.

In arrangements in which the local Bedoop system is redirected, by the DNS leaf node server, to a further server that actually handles the response, access to the further server may be through a port 59 (e.g., a special URL) tailored to receipt of Bedoop data.

In a typical implementation, most or all of the servers are mirrored, or otherwise replicated/redundant, so that failure of individual computers does not impair operation of the system.

Caching can be provided throughout the trees of servers to speed responses. That is, responses by leaf nodes for certainly commonly-encountered CLASS/DNS IDs can be temporarily stored earlier in the tree(s). Bedoop data, propagating through the server network, can prompt a response from an intermediate server if there is a cache hit.

If desired, Bedoop traffic through the above-detailed server trees can be monitored to collect demographic and statistical information as to what systems are sending what Bedoop data, etc. One use of such information is to dynamically reconfigure the DNS network to better balance server loads, to virtually relocate DNS resources nearer regions of heavy usage, etc. Another use of such information is for marketing purposes, e.g., to promote certain Bedoop features and applications within user groups (e.g., internet domains) that seem to under-utilize those features.

Within certain user networks that are linked to the internet, e.g., corporate networks, Bedoop data that isn't handled within the originating Bedoop system may first be routed to a Bedoop name server within the corporate network. That server will recognize certain types of Bedoop data, and know of resources within the corporate network suitable for handling same. Referral to such resources within the corporate network will be made, where possible. These resources (e.g., corporate servers) may respond to Bedoop data in a way customized to the corporate preferences. If the corporate Bedoop name server does not know of a resource within the corporate network that can respond to the Bedoop data, the corporate name server then routes the data to the public Bedoop network described above. (Such referral can be to the master registration server or, to the extent the corporate name server knows the addresses of appropriate servers within the DNS server tree, or of the further servers to which DNS servers may point for certain Bedoop data, it can redirect the local Bedoop system accordingly.)

In typical rich Bedoop implementations, local systems may have libraries of Bedoop services, applications, or protocols. Some may be unique to that computer. Others may be commonly available on all computers. Some may be highly secure, employing encryption and/or anti-hacking measures, or data protocols that are not generally recognized. Others may be shareware, or the result of open-source programming efforts.

While the just-described arrangements used a 12/24/24 bit protocol for CLASS/DNS/UID data, other arrangements can of course be used. In some applications it is advantageous for the protocol to more nearly match those commonly used for internet communications. For example, IP addresses for internet Domain Name Servers (DNS) are presently 32 bits, with extension to 64 or 128 bits foreseen in the near future. The DNS field in Bedoop systems can be follow the internet standard.

Greeting Cards, Birthday Cards, Etc.

To further illustrate some of the basic principles associated with this technology, consider greeting cards and the like that are encoded (e.g., by texturing, printing, etc.) with Bedoop data. On receiving such a card, a recipient holds it in front of the image capture device on a laptop or other computer. The computer responds by displaying an internet web page that has a stock- or customized-presentation (image, video, audio-video, etc.) to complement that presented on the greeting card.

The web site presentation can be personalized by the sender (e.g., with a text message, recent family photographs, etc.), either at the point of card sale, or sometime after the card is purchased. In the latter case, for example, the card can be serialized. After taking the card home, the purchaser can visit the card vendor's web site and enter the card serial number in an appropriate user interface. The purchaser is then presented with a variety of simple editing tools to facilitate customization of the web greeting. When the sender is finished designing the web greeting, the finished web page data is stored (by software at the vendor's web site) at a site corresponding to the serial number.

When the card is received by a recipient and held in front of a Bedoop sensor, CLASS, DNS, and UID data is decoded from the card. The CLASS and DNS data are used to navigate the earlier-described server network to reach a corresponding DNS leaf node server (perhaps maintained by the Hallmark greeting card company). That leaf node server indexes a table, database, or other data structure with the UID from the Bedoop data, and obtains from that data structure the address of an ultimate web site – the same address at which the web greeting customized by the sender was stored. That address is provided by the DNS leaf node server back to the local computer, with instructions that the web page at that address be loaded and displayed (e.g., by HTML redirection). The local computer complies, presenting the customized web greeting to the card recipient.

In the just-described embodiment, in which a pre-encoded card is purchased by a sender and the web-display is then customized, the address of the web site is typically determined by the card vendor. But this need not be the case. Likewise, the card need not be "purchased" in the typical, card-shop fashion.

To illustrate the foregoing alternatives, consider the on-line acquisition of a greeting card, e.g., by visiting a web site specializing in greeting cards. With suitable user-selection (and, optionally, customization), the desired card can be printed using an ink-jet or other printer at the sender's home. In such case, the Bedoop data on the card can be similarly customized. Instead of leading to a site determined by the card vendor, the data can lead to the sender's personal web page, or to another arbitrary web address.

To effect such an arrangement, the sender must arrange for a DNS leaf node server to respond to a particular set of Bedoop data by pointing to the desired web page. While individuals typically will not own DNS servers, internet service providers commonly will. Just as AOL provides simple tools permitting its subscribers to manage their own modest web pages, internet service providers can likewise provide simple tools permitting subscribers to make use of DNS leaf node servers. Each subscriber may be assigned up to 20 UIDs. The tools would permit the users to define a corresponding web address for each UID. Whenever a Bedoop application led to that DNS leaf node server, and presented one of those UIDs, the server would instruct the originating computer to load and present the web page at the corresponding web address.

Prior to customizing the greeting card, the sender uses the tool provided by the internet service provider to store the address of a desired destination web address in correspondence with one of the sender's available UIDs. When customizing the greeting card, the sender specifies the Bedoop data that is to be encoded, including the just-referenced UID. The greeting card application encodes this data into the artwork and prints the resulting card. When this card is later presented to a Bedoop system by the recipient, the recipient's system loads and displays the web page specified by the sender.

<u>*Commerce in Bedoop Resources*</u>

In the just-described arrangement, internet service providers make available to each subscriber a limited number of UIDs on a DNS server maintained by the service. Business enterprises typically need greater Bedoop resources, such as their own DNS IDs (or even their own CLASS ID(s).

While variants of the Bedoop system are extensible to provide an essentially unlimited number of CLASS IDs and DNS IDs, in the illustrated system these resources are limited. Public service, non-profit, and academic applications should have relatively generous access to Bedoop resources, either without charge or for only a modest charge. Business enterprises, in contrast, would be expected to pay fees to moderate their potentially insatiable demand for the resources. Small businesses could lease blocks of UIDs under a given CLASS/DNS ID. Larger businesses could acquire rights to entire DNS IDs, or to entire CLASS IDs (at commensurately greater fees).

Web-based systems for assigning DNS IDs (and CLASS IDs) can be modeled after those successfully used by Internic.com, and now Networksolutions.com, for registration of internet domains. The user fills out a web-based form with names, addresses, and billing information; the system makes the

necessary changes to all of the hidden system infrastructure – updating databases, routing tables, etc., in servers around the world.

Controlled-Access ID

Just as the above-described embodiment employed an ink-jet printer to produce a customized-Bedoop greeting card, the same principles can likewise be applied to access-control objects, such as photo-IDs.

Consider an employment candidate who will be interviewing at a new employer. The candidate's visit is expected, but she is not recognized by the building's security personnel. In this, and many other applications, arrangements like the following can be used:

The employer e-mails or otherwise sends the candidate an access code. (The code can be encrypted for transmission.) The code is valid only for a certain time period on a given date (e.g., 9:00 a.m. – 11:00 a.m. on June 28, 1999).

Upon receipt of the access code, the candidate downloads from the web site of the state Department of Motor Vehicles the latest copy of her driver's license photo. The DMV has already encoded this photo with Bedoop data. This data leads to a state-run DNS leaf node server 56. When that server is presented with a UID decoded from a photograph, the server accesses a database and returns to the inquiring computer a text string indicating the name of the person depicted by the photograph.

The candidate incorporates this photo into an access badge. Using a software application (which may be provided especially for such purposes, e.g., as part of an office productivity suite such as Microsoft Office), the photo is dragged into an access badge template. The access code emailed from the employer is also provided to this application. On selecting "Print," an ink-jet printer associated with the candidate's computer prints out an access badge that includes her DMV photo and her name, and is also steganographically encoded in accordance with the employer-provided access code.

The name printed on the badge is obtained (by the candidate's computer) from the DMV's DNS server, in response to Bedoop data extracted from the photograph. (In this application, unlike most, the photograph is not scanned as part of a Bedoop process. Instead, the photograph is already available in digital form, so the Bedoop decoding proceeds directly from the digital representation.)

For security purposes, the access code is not embedded using standard Bedoop techniques. Instead, a non-standard format (typically steganographic) is employed. The embedding of this access code can span the entire face of the card, or can be limited to certain regions (e.g., excluding the region occupied by the photograph).

On the appointed day the candidate presents herself at the employer's building. At the exterior door lock, the candidate presents the badge to an optical sensor device, which reads the embedded building access code, checks it for authenticity and, if the candidate arrived within the permitted hours, unlocks the door.

Inside the building the candidate may encounter a security guard. Seeing an unfamiliar person, the guard may visually compare the photo on the badge with the candidate's face. Additionally, the guard can present the badge to a portable Bedoop device, or to one of many Bedoop systems scattered through the building (e.g., at every telephone). The Bedoop system extracts the Bedoop data from the card (i.e., from the DMV photograph), interrogates the DMV's DNS server with this Bedoop data, and receives in reply the name of the person depicted in the photograph. (If the Bedoop system is a telephone, the name may be displayed on a small LCD display commonly provided on telephones.)

The guard checks the name returned by the Bedoop system with the name printed on the badge. On seeing that the printed and Bedoop-decoded names match (and optionally checking the door log to see that a person of that name was authorized to enter and did so), the security guard can let the candidate pass.

It will be recognized that the just-described arrangement offers very high security, yet this security is achieved without the candidate ever previously visiting the employer, without the employer knowing what the candidate looks like, and by use of an access badge produced by the candidate herself.

Variants of such home-printed badge embodiments find numerous applications. Consider purchasing movie- or event-tickets over the web. The user can print an access ticket that has an entry code embedded therein. On arriving at the theater or event, the user presents the ticket to an optical scanning device, which decodes the entry code, checks the validity of same, authorizes the entry, and marks that entry code as having been used (preventing multiple uses of tickets printed with the same code).

Another Controlled Access ID

A great variety of access control systems can be implemented using the present technology. The foregoing is just one example.

Another application employs an ID card, Bedoop technology, and proximity detection technology (commonly known as RFID).

The ID card can be a badge or the like having a steganographically-encoded photograph of the bearer. The card further includes a proximity ID device, such as an unpowered electronic circuit that is excited and detected by a radiant field from an associated proximity detector, providing a unique signature signal identifying a particular individual.

The building can be provided with an image sensor (such as a video camera or the like), an associated Bedoop detection system, and the proximity detector. When a user wearing the badge approaches, the proximity detector signals the camera to capture image data. The Bedoop detection system identifies the badge photograph (e.g., by clues as are described in the prior applications, or without such aids), captures optical data, and decodes same to extract the steganographically-embedded data hidden therein. The access control system then checks whether the badge ID discerned from the proximity sensor

properly corresponds to the Bedoop data extracted from the photograph on the badge. If so, access is granted; if not, the data is logged and an alarm is sounded.

By such arrangement, premises security is increased. No longer can proximity-based access badges be altered to substitute the picture of a different individual. If the photo is swapped, the proximity system ID and the embedded photo data will not match, flagging an unauthorized attempted access.

The same principles are applicable in many other contexts – not limited to RF-based proximity detection systems. For example, the data decoded from the photograph can be compared against other forms of machine-sensed personal identification associated with the badge. These include, but are not limited to, bar code IDs, mag-stripe ID cards, smart cards, etc. Or the comparison can be with an identification metric not associated with the badge (e.g., retinal scan, voice print, or other biometric data).

Ink-Jet Printing

In the foregoing discussions, reference has been made to use of ink-jet printing as a means for providing steganographically encoded indicia on substrates. The following discussion expands on some of the operative principles.

The basic physics and very low level analog electronic operation of ink-jet printers (sometimes termed bubble-jet printers) are ideally suited to support very-light-tint background digital watermarking on any form of substrate. (Watermarking through apparent "tinting" of substrates is discussed in published specification WO0007356, corresponding to US application 09/127,502.) In general, the statement, "if you can print it with an ink jet printer, you can watermark it" is largely accurate, even for (perhaps especially for) simple text documents. Indeed, there is a degree of flexibility and control in the ink-jet printing realm that is not as generally available in more traditional printing technologies, such as commercial offset printing and other plate-based technologies. (This is not to say that ink-jet has better quality than plate-based technologies; it has more to do with the statistics of ink droplets than anything else.) Heavier tint backgrounds are possible as well, where the continuum ranges from very light background tinting, where the casual observer will see "white paper," all the way through heavily inked patterned backgrounds, and photographs themselves, and everything in between.

In some embodiments, the ink-jet driver software is modified to provide lower-level control of individual droplet emission than is provided in existing printer drivers, which are naturally optimized for text and graphics. In some such embodiments, the "watermarking" print mode is another option from which the user can select (e.g., in addition to High Quality, Econo-Fast, etc.), or the selection can be made automatically by application software that is printing watermarked data.

In more sophisticated embodiments, the watermark data is applied to the printer driver software independently of the other image/text data. The printer driver is arranged to eject droplets in the usual print density for the image/text data, and at a more accurately-controlled, finer density for the separately-applied watermark data. (The latter may be effected as a slight modulation signal on the former.) This

arrangement provides for essentially transparent integration into existing printer environments – no one need worry about the watermarking capability except the software applications that specifically make use of same.

Consumer Marking of Web-Based Materials

Various items of printed media can originate off the web, yet be printed at home. Examples include movie tickets, coupons, car brochures, etc. Bedoop data can be added, or modified, by the software application or by the printer driver at the time of printing. (Alternatively, the Bedoop data can be customized to correspond to the user before being downloaded to the user's system for printing.)

One advantage to Bedoop-encoding printed images locally, as opposed to Bedoop-encoding the image files prior to downloading for local printing, is that the encoding can be tailored in accordance with the particular properties of the local printer (e.g., to increase robustness or decrease visibility) – properties not generally known to a remote server.

In one particular example, the UID field in the Bedoop data can be written with a value that serves as an index to a database of user profiles, permitting later systems to which the printed item is presented to personalize their response in accordance with the profile data.

In another example, the UID field serves an authentication purpose, e.g., to verify that the printed medium actually was printed at a particular place, or by a particular user or at a particular time.

Coffee Mug

At retail coffee outlets, customers commonly order the same drink day after day ("half-decaf, short, skinny latte"). Some customers present personal coffee mugs to the cashier, preferring the sensation of ceramic or metal to paper, and avoiding the trash/recycle dilemma.

The drinker's "regular" order can be Bedoop-encoded either on the mug itself or, more commonly, on an adhesive label applied to the mug. The encoding can be in addition to other aesthetic imagery (e.g., artwork or a photo), or the marking can be purely data. Labels the size of postage stamps may be used.

On handing the mug to the cashier, the customer can simply say "the regular." The cashier passes the mug in front of the optical scanning device of a Bedoop system associated with the cash register. The system steganographically decodes the data and provides the corresponding order ("half-decaf, short, skinny latte"), either textually or audibly (e.g., by a voice synthesizer) to the cashier or the barrista. The cash register system also knows the current price of the requested drink, and rings up the charge accordingly.

Labels of the type described can be available to the cashier on pre-printed rolls, just as with other adhesive stickers, or can be printed on-demand. (Small label printers may be best suited in the latter case,

given space constraints in retail outlets.) Customers ordering drinks for personal mugs may be invited to take a label corresponding to their just-ordered drink and apply it to their mug for future use.

In variants on this basic theme, the mug label can be further encoded (or a supplemental label can be provided and encoded) with electronic payment information, such as the customer's credit card number, or the number of a debit account maintained by the coffee merchant for that customer. When the mug is scanned for the drink order, the system likewise detects the payment information and charges the corresponding fee to the appropriate account. (For security reasons, the system may be arranged so that the mug cannot be used to authorize more than, say $5 of coffee drink purchases per day.)

In another variant on this theme, the system maintains an electronic log of coffee purchases made by the customer and, in accordance with then-prevailing marketing considerations, rewards the customer with a free drink after 8 or 12, etc., drinks have been purchased.

In still another variant on this theme, regular customers who use Bedoop-labeled mugs can participate in periodic promotions in which, for example, every N^{th} such customer is rewarded with a cash or merchandise prize. Bells go off when the N^{th} mug is scanned. (N can be a fixed number, such as 500, or can be a random number – typically within a known range or with a known mean.)

<u>*Warping and Focus Issues*</u>

The coffee cup is an example of a non-planar object. Another is soft drink cans. Special issues can arise when encoding and decoding markings on such objects. For example, when sensing such an object with a camera or the like, part of the image will be out of focus due to differing distances from the camera to different parts of the can surface.

While parts of an image sensed from a non-planar object, such as a can, may be out of focus, they still convey useful image data. The out of focus areas are just blurred – as if filtered by a low pass filter. But to make use of this information, a further complication must first be addressed: warping.

When viewed from a camera, the planar artwork with which the can is wrapped becomes warped. Portions of the can nearest the camera appear at a nominal full scale, while areas successively further around the can curvature (as viewed from the camera) appear progressively more and more spatially compressed. Regardless of the watermarking technology being employed, the physical warp of the can's surface is likewise manifested as a warping of the encoded watermark data.

On way of handling this issue is to pre-warp the watermark pattern to account for this optical distortion.

In watermarking techniques that operate directly on luminance values, the grid by which the watermark is applied can be pre-distorted to counteract the subsequent optical distortion of the artwork as it is perceived on the cylindrical can. Consider a Pepsi or Coke can. A virtual center line may pass through the center of the logo artwork (the "front" of the can), and serves as a center line of one of the watermark gridded tiles. On either side of this center line the grid is successively stretched. This

stretching is computed so that, when viewed by a camera, the watermark grid has the appearance of being uniformly rectilinear, instead of being successively compressed towards the apparent edge of the can, as would otherwise be the case.

An illustration of such an approach is shown in the Figures. Fig. 17 shows an unwarped grid – as would commonly be used in watermarking planar objects. Fig. 18 shows the same grid – prewarped to account for optical distortion due to can curvature. The artwork (e.g., label) center-line is shown by the dotted lines.

More typically the grid is square rather than rectangular. Moreover, the illustrated distortion contemplates that the depicted grid spans +/- 90 degrees from the can front. Also, the grid is typically smaller (e.g., one inch on a side), so several grids are tiled adjacent each other in a span of +/- 90 degrees.) Still further, the illustrated pre-warping is based on an infinite projection (i.e., the can surface as viewed from a distance of infinity – encompassing a full +/- 90 degrees from the center line). More typically, the warp would be computed based on a finite projection – using a typical lens-to-object distance (e.g., 2-24 inches), resulting in a view that encompasses less than a full +/- 90 degree range from the center line.

The illustrated grid is pre-warped only in the horizontal direction, and only in accordance with a curvature-induced geometrical distortion. Another apparent geometrical distortion is also present – one due to different parts of the can being further from the camera. The further away, the smaller the appearance. Accordingly, grid elements expected to be positioned further from the camera should be made commensurately larger in order to pre-compensate for this distance-induced geometrical distortion. Such distance-induced geometrical distortion is manifested equally in the horizontal and vertical directions. Thus, a more accurate pre-warp would also progressively swell the grid cells both in vertical and horizontal dimensions at progressive displacements from the center line, so as to counter-act the further-looks-smaller effect. Fig. 19 shows the basic nature of such a pre-warp.

The degree of this latter pre-warping will be heavily dependent on the distance from the camera lens to the front of the can. If the distance is on the order of two inches, the further-looks-smaller effect will be much more pronounced that if the distance is a foot or more. In the latter case, the distance to the most remote portion of the imaged object may be 110% the distance to the closest portion, whereas in the former case, the ratio may be more on the order of 200%.

The illustrated pre-warping is exemplary of that which may be applied when the watermark is applied in the pixel domain using a grid pattern. It is geometrical pre-warping – i.e., in the spatial domain. Other watermarking approaches would naturally require pre-warping of other sorts, corresponding to the anticipated warping of the watermark data representation. For example, watermarking techniques that rely on changing image coefficients in transformed domains would require different adjustments. Conceptually these adjustments are the same (i.e., resulting in an apparent image having the intended watermark information), but the manifestation is not susceptible to illustration like that given in Figs. 17

and 18 (i.e., since transform coefficients are being changed - rather than grid layout, warping in a transform domain - rather than in a spatial domain, would be required).

Although the foregoing description focused on pre-warping the image, the problem can be handled otherwise. If a rectilinear watermark – not pre-warped – is applied to a cylindrical can, the watermark detector can apply an unwarping operation to counteract the applicable distortion. That is, the detector can virtually remap the raw pixel data to effectively stretch the pixels away from the center line to restore them to their proper rectilinear relationship.

In one embodiment, the sensed image data is first trial-decoded without unwarping – assuming the imaged subject is planar. If no watermark is detected, the same data (or a subsequent frame of image data) is trial-unwarped to see if perhaps the data so yields a readable watermark. Several successive unwarpings of different characters may be tried. In some embodiments, a detector may continuously cycle through several different unwarping functions (including no unwarping) to try and happen on an unwarping function that permits a watermark be discerned from the image data.

If the application permits, the user may specify the shape of the object so that a single, or limited range, of unwarping functions is applied. Or the user can simply provide a gross cue to the detector (e.g., by selecting between "magazines" or "grocery products' on a user interface associated with the watermark detector). In the former case, the medium is known to be flexible and may assume random simple curvatures other than planar. In such case the detector may spend most of its time trying to decode the watermark assuming the imaged page is planar, and occasionally try applying one of four or eight different unwarping functions as would be appropriate if the magazine page were slightly drooping in different directions. In the latter case, grocery products are generally fairly unflexible and thus have relatively predictable shapes - most commonly planar or cylindrical. In such case the detector may spend half its time trying to decode assuming the object is planar, and spend the other half of its time cycling among a variety of cylindrical unwarping functions.

While the foregoing discussion particularly addressed image watermarking, counterparts of these principles are likewise applicable to audio watermarking.

Smart Elevators

In accordance with another embodiment, a building elevator is provided with one or more optical capture devices. Each device examines monitors the contents of the elevator chamber, looking for Bedoop encoded objects, such as ID badges.

On sensing a Bedoop-encoded object, the elevator can determine – among other data – the floor on which the wearer's office is located. The system can then automatically direct the elevator to that floor, without the need for the person to operate any buttons. (The elevator's button panel can be provided with a new, override button that can be operated to un-select the most recently selected floor(s), e.g., in case a user wants to travel to a different floor.)

To aid in identification, the Bedoop objects (e.g., badges) can be colored a distinctive color, permitting the system to more easily identify candidate objects from other items within the optical capture devices' field of view. Or the object can be provided with a retro-reflective coating, and the elevator can be equipped with one or more illumination sources of known spectral or temporal quality (e.g., constant infra red, or constant illumination with a single- or multi-line spectrum, or a pulsed light source of known periodicity; LEDs or semiconductor lasers, each with an associated diffuser, can be used for each the foregoing and can be paired with the image capture devices). Other such tell-tale clues can likewise be used to aid in object location. In all such cases, the optical capture device can sense the tell-tale clue(s) using a wide field of view sensor. The device can then be physically or electronically steered, and/or zoomed, to acquire a higher resolution image of the digitally-encoded object suitable for decoding.

Magazines

Magazine (and newspaper) pages can be steganographically encoded with Bedoop data to provide another "paper as portal" experience. As with the earlier-described office document case, the encoded data yields an address to a computer location (e.g., a web page) having the same, or related, content.

In one exemplary embodiment, the blank magazine page stock is Bedoop-encoded prior to printing. The watermarking can be performed by high speed ink-jet devices, which splatter a fine pattern of essentially imperceptible ink droplets across each page. Each page can be differently watermarked so that, on decoding, page 21 of a magazine can be distinguished from page 22 of the same magazine (and page 106 of the June 21, 1999, issue can be distinguished from page 106 of the June 28, 1999, issue). If desired, each page can be further segregated into regions – either in accordance with the actual boundaries of articles that will later be printed on the pages, or in a grid pattern, e.g., of 3 columns across by 5 rows high. Each region conveys a distinct Bedoop code, permitting different portions of the page to lead to different web data.)

After watermarking and printing, the pages thus produced are bound in the usual fashion with others to form the finished magazine. (Not all pages in the magazine need to be watermarked.)

Of course, the watermarking can be effected by processes other than ink-jet printing. For example, texturing by pressure rollers is another option well suited for the large volumes of paper to be processed. Or the artwork presented in the advertisement can be digitally watermarked using commercial watermarking software (as is available, e.g., with Adobe Photoshop and Corel image editing products).

On presenting a magazine to the optical scanner device of a Bedoop-compliant computer, the computer senses the Bedoop data, decodes same, and launches a web browser to an internet address corresponding to the Bedoop data. If the magazine page is an advertisement, the internet address can provide information complementary to the advertisement. For example, if the magazine page is an advertisement for a grocery item, the Bedoop data can identify a web page on which recipes that make use

of the advertised item are presented. If the magazine page includes a photo of a tropical beach, the Bedoop data can lead to a travel web page (e.g., hosted by Expedia or other travel enterprise) that presents fare and lodging information useful to a reader who wants to vacation at the illustrated beach. (The fare information can be customized to the reader's home airport by reference to user profile data stored on the user's computer and relayed to the web site to permit customization of the displayed page.)

The data to which the Bedoop data leads needn't be static; it can be updated on a weekly, daily, or other basis. Thus, if a months-old magazine page is presented to a Bedoop device, the resultant data can be up-to-the-minute. The linked data can include audio and/or video presentations.

In the case of advertising, the inclusion of Bedoop data increases the value of the ad to the advertiser, and so merits a higher charge to the advertiser from the magazine publisher. This higher charge may be shared with the enterprise(s) that provides the Bedoop technology and infrastructure through which the higher value is achieved.

Business Card Applications

Conventional business cards can be steganographically encoded with Bedoop data, e.g., by texturing, watermark tinting, ink-jet splattering, text steganography, etc. As with many of the earlier-described embodiments, the steganographic encoding is tailored to facilitate decoding in the presence of arbitrary rotation or scale distortion of the card introduced during scanning. (Some such techniques are shown, e.g., in applicant's earlier patents and publications identified above. Various other techniques are known to artisans.)

When a recipient of a business card holds it in front of a Bedoop sensor, the operating system on the local system launches a local Bedoop application. That local Bedoop application, in turn, establishes an external internet connection to a remote business card server. The address of that server may already be known to the local Bedoop application (e.g., having been stored from previous use), or the local Bedoop system can traverse the above-described public network of DNS servers to reach the business card server.

A database on the business card name server maintains a large collection of business card data, one database record per UID. When that server receives Bedoop data from a local Bedoop system, it parses out the UID and accesses the corresponding database record. This record typically includes more information than is commonly printed on conventional business cards. Sample fields from the record may include, for example, name, title, office phone, office fax, home phone, home fax, cellular phone, email address, company name, corporate web page address, personal web page address, secretary's name, spouse's name, and birthday. This record is transmitted back to the originating Bedoop system.

The local Bedoop system now has the data, but needs further instruction from the user as to how it should be processed. Should a telephone number be dialed? Should the information be entered into a personal contact manager database (e.g., Outlook) on the local system? Etc.

In an exemplary embodiment, the local system presents the available choices to the user, e.g., by textual prompts, synthesized voice, etc. The user responds by manipulating the business card in a manner prompted by the system (e.g., move down to telephone office; move up to telephone at home; move right to access corporate web page; move left to access personal web page; rotate left to enter certain elements from the database record (filtered in accordance with a template) into personal contact manager database, etc.. The local Bedoop system responds accordingly.

Some card givers may choose to make additional information available to card recipients -- information beyond that known in prior art contact-management software applications. For example, one of the choices presented by a local Bedoop system in response to presentation of a business card may be to review the card-giver's personal calendar. (The card-giver can maintain his or her personal calendar on a web-accessible computer.) By such arrangement, the card-recipient can learn when the card-giver may be found in the office, when appointments might be scheduled, etc., etc.

Typically, access to this web-calendar is not available to casual web browsers, but is accessible only in response to Bedoop data (which may thus be regarded as a form of authentication or password data).

Some users may carry several differently-encoded cards, each with a different level of access authorization (e.g., with different UIDs). Thus, some cards may access a biographical page without any calendar information, other cards may access the same or different page with access enabled to today's calendar, or this week's calendar, only, and still other cards (e.g., the "spouse" card) may access the same or different page with access enabled for the card-giver's complete calendar. The user can distribute these different cards to different persons in accordance with the amount of personal information desired to be shared with each.

In accordance with a related embodiment, the database record corresponding to Bedoop business card data can include a "now" telephone number field. This field can be continually-updated throughout the day with the then-most-suitable communications channel to the card-giver. When the card-giver leaves home to go to the office, or leaves the office for a trip in the car, or works a week at a corporate office in another town, etc., this data field can be updated accordingly. (A pocket GPS receiver, with a wireless uplink, can be carried by the person to aid in switching the "now" number among various known possibilities depending on the person's instantaneous position.) When this database record is polled for the "now" number, it provides the then-current information.

Consider a Bedoop-enabled public telephone. To dial the phone, a business card is held in front of the Bedoop sensor (or slid through an optical scanner track). The phone interrogates the database at the business card server for the "now" number and dials that number.

To update the any of the fields stored in the database record, the card giver can use a special card that conveys write-authorization privileges. This special card can be a specially encoded version of the business card, or can be another object unique to the card-giver (e.g., the card-giver's driver's license).

The reference to business cards and personal calendars is illustrative only. Going back a century, "calling cards" were used by persons whose interests were strictly social, rather than business. The just-discussed principles can be similarly applied. Teenagers can carry small cards to exchange with new acquaintances to grant access to private dossiers of personal information, favorite music, artwork, video clips, etc. The cards can be decorated with art or other indicia that can serve purposes wholly unrelated to the Bedoop data steganographically encoded therein.

Gestural Input

A Bedoop system can determine the scale state, rotation state, X-Y offset, and differential scale state, of an object by reference to embedded calibration data, or other techniques. If the scan device operates at a suitably high frame rate (e.g., five or ten frames per second), change(s) in any or all of these four variables can be tracked over time, and can serve as additional input.

In an earlier-discussed example, moving an object to the left or right in front of the Bedoop scanner caused a left- or right-positioned button in a dialog box to be selected. This is a change in the X-Y offset of the scanned object. In that earlier example, moving the object inwardly towards the camera caused the selected button to be activated. This is a change in the scale state of the scanned object.

In similar fashion, twisting the object to the left or right can prompt one of two further responses in a suitably programmed Bedoop application. (This is a change in the rotation state.) Likewise, tilting the object so that one part is moved towards or away from the camera can prompt one of two further responses in the application. (This is a change in the differential scale state.)

In the business card case just-discussed, for example, the card can be held in front of the Bedoop scanner of a computer. If the card is twisted to the left, the computer opens a web browser to a web page address corresponding to Bedoop data on the card. If the card is twisted to the right, the computer opens an e-mail template, pre-addressed to an e-mail address indicated by the card.

In other examples, twisting an object to move the right edge towards the scanner can be used to effect a right mouse click input, and twisting the object to move the right edge away from the scanner can be used to effect a left mouse click input.

Simultaneous changes in two of these four positioning variables can be used to provide one of four different inputs to the computer (e.g., (a) twisting left while moving in; (b) twisting left while moving out; (c) twisting right while moving in; and (d) twisting right while moving out). Simultaneous changes to three or all four of these variables can similarly be used to provide one of eight or sixteen different inputs to the computer.

Simultaneous manipulations of the object in two or more of these modes is generally unwieldy, and loses the simple, intuitive, feel that characterizes manipulation of the object in one mode. However, a similar effect can be achieved by sequential, rather than simultaneous, manipulation of the card in different modes (e.g., twist left, then move in). Moreover, sequential manipulations permit the same mode to be used

twice in succession (e.g., move in, then move out). By such sequential manipulations of the object, arbitrarily complex input can be conveyed to the Bedoop system.

(It will be recognized that a digitally-encoded object is not necessary to the gestural-input applications described above. Any object (talisman) that can be distinguished in the image data can be manipulated by a user in the manners described above, and an appropriate system can recognize the movement of the object and respond accordingly. The provision of digital data on the object provides a further dimension of functionality (e.g., permitting the same gesture to mean different things, depending on the digital encoding of the object being manipulated), but this is not essential.

Moreover, even within the realm of digitally-encoded gestural talismans, steganographic encoding is not essential. Any other known form of optically-recognizable digital encoding (e.g., 1D and 2D bar codes, etc.) can readily be employed.

In an illustrative embodiment, a business card or photograph is used as the talisman, but the range of possible talismans is essentially unlimited.

Dynamic gestures are not the only communications that can be effected by such talismans. Static positioning (e.g., presenting the talisman at different orientations) can alternatively be employed.

Consider a magazine advertisement. When presented to the sensor with the top of the page up, a first response can be invoked. If the page is presented at a rotation of 90 degrees, a second response can be invoked. Similarly with 180 degrees rotation (i.e., upside down), and 270 degrees rotation. The Bedoop detector can detect these different rotational states by reference to attributes of the watermark signal discerned from the magazine page (e.g., by reference to the rotation state discerned from the subliminal grid signal detailed in applicant's prior patents).

Gestural Decoding Module

There are various ways in which the Bedoop system's decoding of gestural input can be effected. In some Bedoop systems, this functionality is provided as part of the Bedoop applications. Generally, however, the applications must be provided with the raw frame data in order to discern the gestural movements. Since this functionality is typically utilized by many Bedoop applications, it is generally preferable to provide a single set of gestural interpretation software functions (commonly at the operating system level) to analyze the frame data, and make available gestural output data in standardized form to all Bedoop applications.

In one such system, a gestural decoding module tracks the encoded object within the series of image data frames, and outputs various parameters characterizing the object's position and manipulation over time. Two of these parameters indicate the X-Y position of the object within current frame of image data. The module can identify a reference point (or several) on the object, and output two corresponding position data (X and Y). The first represents the horizontal offset of the reference point from the center of the image frame, represented as a percentage of frame width. A two's complement representation, or other

representation capable of expressing both positive and negative values, can be used so that this parameter has a positive value if the reference point is right of center-frame, and has a negative value if the reference point is left of center frame. The second parameter, Y, similarly characterizes the position of the reference point above or below center-frame (with above-being represented by a positive value). Each of these two parameters can be expressed as a seven-bit byte. A new pair of X, Y parameters is output from the gestural decoding module each time a new frame of image data is processed.

In many applications, the absolute X-Y position of the object is not important. Rather, it is the movement of the object in X and Y from frame-to-frame that controls some aspect of the system's response. The Bedoop application can monitor the change in the two above-described parameters, frame to frame, to discern such movement. More commonly, however, the gestural decoding module performs this function and outputs two further parameters, X' and Y'. The former indicates the movement of the reference point in right/left directions since the last image frame, as a percentage of the full-frame width. Again, this parameter is represented in two's complement form, with positive values representing movement in the rightward direction, and negative values representing movement in the leftward direction. The later parameter similarly indicates the movement of the reference point in up/down directions since the last frame.

The scale, differential scale, and rotation states of the object can be similarly analyzed and represented by parameters output from the gestural decoding module.

Scale state can be discerned by reference to two (or more) reference points on the object (e.g., diagonal corners of a card). The distance between the two points (or the area circumscribed by three or more points) is discerned, and expressed as a percentage of the diagonal size of the image frame (or its area). A single output parameter, A, which may be a seven-bit binary representation, is output.

As with X-Y data, the gestural decoding module can likewise monitor changes in the scale state parameter since the last frame, and product a corresponding output parameter A'. This parameter can be expressed in two's complement form, with positive values indicating movement of the object towards the sensor since the last frame, and negative values indicating movement away.

A differential scale parameter, B, can be discerned by reference to four reference points on the object (e.g., center points on the four edges of a card). The two points on the side edges of the card define a horizontal line; the two points on the top and bottom edges of the card define a vertical line. The ratio of the two line lengths is a measure of differential scale. This ratio can be expressed as the shorter line's length as a percentage of the longer line's length (i.e., the ratio is always between zero and one). Again, a two's complement seven-bit representation can be used, with positive values indicating that the vertical line is shorter, and negative values indicating that the horizontal line is shorter. (As before, a dynamic parameter B' can also be discerned to express the change in the differential scale parameter B since the last frame, again in two's complement, seven bit form.)

A rotation state parameter C can be discerned by the angular orientation of a line defined by two reference points on the object (e.g., center points on the two side edges of a card). This parameter can be encoded as a seven-bit binary value representing the percentage of rotational offset in a clockwise direction from a reference orientation (e.g., horizontal). (The two reference points must be distinguishable from each other regardless of angular position of the object, if data in the full range of 0 – 360 degrees is to be represented. If these two points are not distinguishable, it may only be possible to represent data in the range of 0-180 degrees.) As before, a dynamic parameter C' can also be discerned to express the change in the rotation state parameter C since the last frame. This parameter can be in seven bit, two's complement form, with positive values indicating change in a clockwise rotation

The foregoing analysis techniques, and representation metrics, are of course illustrative only. The artisan will recognize many other arrangements that can meet the needs of the particular Bedoop applications being served.

In the illustrative system, the Bedoop application programs communicate with the gestural decoding module through a standardized set of interface protocols, such as APIs. One API can query the gestural input module for some or all of the current position parameters (e.g., any or all of X, Y, A, B, and C). The module responds to the calling application with the requested parameter(s). Another API can query the gestural input module for some or all of the current movement data (e.g., any or all of X', Y', A', B' and C'). Still another API can request the gestural decoding module to provide updated values for some or all of the position or movement data on a running basis, as soon as they are discerned from each frame. A complementary API discontinues the foregoing operation. By such arrangement, all of the gestural data is available, but the Bedoop application programs only obtain the particular data they need, and only when they ask for it.

In Bedoop applications that communicate with external servers, just the Bedoop data (i.e., CLASS, DNS, and optionally UID) may initially be sent. If the remote server needs to consider gestural data in deciding how to respond, the remote server can poll the local Bedoop system for the necessary data. The requested gestural data is then sent by the local Bedoop system to the remote server in one or more separate transmissions.

In other embodiments, since the gestural data is of such low bandwidth (e.g., roughly 56 bits per image frame), it may routinely and automatically be sent to the remote computer, so that the gesture data is immediately available in case it is needed. In an illustrative implementation, this data is assembled into an 8-byte packet, with the first byte of the packet (e.g., the X parameter) being prefixed with a "1" sync bit, and subsequent bytes of the packet being prefixed with "0" sync bits. (The sync bits can be used to aid in accurate packet decoding.)

In some embodiments, it is useful to provide for an extension to the normal 64-bit Bedoop length to accommodate an associated packet of gestural data. This can be effected by use of a reserved bit, e.g., in the UID field of the Bedoop packet. This bit normally has a "0" value. If it has a "1" value, that

indicates that the Bedoop data isn't just the usual 64 bits, but instead is 128 bits, with the latter 64 bits comprising a packet of gestural data.

Similar extension protocols can be used to associate other ancillary data with Bedoop data. A different reserved bit in the UID field, for example, may signal that a further data field of 256 bits follows the Bedoop data – a data field that will be interpreted by the remote computer that ultimately services the Bedoop data in a known manner. (Such bits may convey, e.g., profile data, credit card data, etc.) The appended data field, in turn, may include one or more bits signaling the presence of still further appended data.

Grandmothers

It is a common complaint that computers are too complex for most people. Attempts to simplify computer-user interaction to facilitate use by less experienced users usually serve to frustrate more experienced users.

In accordance with this aspect of the present technology, the sophistication of a computer user is steganographically indicated on a talisman used by that user to interact with the system. The computer detects this steganographically-encoded data, and alters its mode of interacting with the user accordingly.

Consider internet browser software. Experienced users are familiar with the different functionality that can be accessed, e.g., by various drop-down menus/sub-menus, by the keyboard shortcuts, by the menus available via right-clicking on the mouse, by manipulating the roller mouse scroll wheel and scroll button, etc., etc. Grandmothers of such users, typically, are not so familiar.

Although gestural interfaces hold great promise for simplifying user-computer interaction, the same dichotomy between experienced users and inexperienced users is likely to persist, frustrating one class of user or the other.

To help close this gap, a computer system can respond to gestures in different manners, depending on the expertise level indicated by encoding of the talisman. For an expert user, for example, the gestural interface active in the internet browser software may display the stored list of Favorite web addresses in response to tipping the left edge of the talisman towards the optical sensor. Once this list is displayed, the expert user may rotate the talisman to the right to cause the highlighting to scroll down the list from the top. Rotating the talisman to the left may scroll the list of Favorites up from the bottom. The speed of scrolling can be varied in accordance with the degree of rotation of the talisman from a default orientation.

In contrast, for the novice user, these talisman manipulations may be confounding rather than empowering. Tipping the left edge of the talisman towards the sensor may occur as often by mistake as on purpose. For such users, a more satisfactory interface may be provided by relying on simple X-Y movement of the talisman to move an on-screen cursor, with a movement of the talisman towards the sensor to serve as a selection signal (i.e., like a left-mouse click).

(In the example just-cited, the expert user summoned a list of Favorite web sites. Different "Favorites" lists can be maintained by the computer – each in association with different talismans. A husband who uses one talisman is provided a different "Favorites" list than a wife who uses a different talisman.)

Printed Pictures

A printed photograph can be steganographically encoded with Bedoop data leading to information relating to the depicted person (e.g., contact information, biographical information, etc.).

Such a photograph can be presented to a Bedoop sensor on a telephone. In a simple embodiment, the telephone simply processes the Bedoop data to obtain a corresponding default telephone number, and dials the number. In other embodiments, various options are possible, e.g., dial home number or dial work number. On presenting the photograph to the telephone, for example, moving the photo to the left may dial the person at home, while moving the photo to the right may dial the person at work.

As telephones evolve into more capable, multi-function devices, other manipulations can invoke other actions. In a computer/telephone hybrid device, for example, rotating the photo counterclockwise may launch a web browser to an address at which video data from a web cam at the pictured person's home is presented. Rotating the photo clockwise may present an e-mail form, pre-addressed to the e-mail address of the depicted person. Moving the photo to the right may query a database on the system for other photographs depicting the same individual or subject, which can be presented in response to further user input. Etc.

In this and other embodiments, it is helpful for the Bedoop device to prompt the user to aid in manipulating the object. This can be done audibly (e.g., "move photo left to dial at home") or by visual clues (e.g., presenting left- or right-pointing arrows).

Bedoop data in photographs can also be used to annotate the photographs, as with notes on the back of a photograph, or printed under the photograph in a photo album. The Bedoop data can lead to a remote database, where the photograph owner is permitted to enter a textual (or audio) narrative in association with each photograph's UID. Years later, when some of the names have been forgotten, the photograph can be positioned in front of a Bedoop sensor, and the system responds by providing the annotation provided by the photograph owner years earlier.

Drivers Licenses and Other Cards

Drivers licenses, social security cards, or other identity documents may be encoded by the issuing authority with Bedoop data that permits access to the holder's personal records over the web. On presenting the document to a Bedoop system, the system directs a web browser to a private address corresponding to data encoded on the document. At that address, the holder of the document can review governmental records, such as state or federal tax return data, social security entitlements, etc., as well as

privately-maintained records, such as credit records, etc. User selection among various functions can be effected by spatial manipulation of the document. (Entry of additional data, such as social security number or mother's maiden name, may be required of the user to assure privacy in case the document is lost or stolen.)

By manipulating a driver's license in front of a Bedoop sensor, a user can request renewal of the driver's license, and authorize payment of the corresponding fee.

Bank cards (debit, credit, etc.) can similarly be encoded with Bedoop data to permit the holder to access bank records corresponding to the bank card account. (Entry of a PIN code may be required to assure privacy.)

Such documents can also be used to access other personal data. One example is e-mail. A traveler might pause at a Bedoop kiosk at an airport and present a driver's license. Without anything more, the kiosk may present email that is waiting for the traveler on an associated display screen.

On recognizing a driver's license, the kiosk can access a remote site (which may be maintained by the Department of Motor vehicles, another government entity, a private entity, or by the traveler), authenticating the operation by presenting Bedoop data encoded on the license, and obtain information that the person has pre-approved for release in response to such authorized access. This information can include e-mail account and password information. Using this information, the kiosk queries the corresponding e-mail server, and downloads a copy of recently received mail for presentation at the kiosk. (A user-entered PIN number may be required at some point in the process, e.g., in querying the remote site for sensitive e-mail password data, before presenting the downloaded e-mail for viewing, etc., to ensure privacy.)

Other cards carried in wallets and purses can also be encoded to enable various functions. The local sandwich shop that rewards regular customers by awarding a free sandwich after a dozen have been purchased can encode their frequent-buyer card with Bedoop data leading to the shop's web-based sandwich delivery service. Or the frequent-buyer card can be eliminated, and customers can instead wave their business card or other identity document in front of the shop's Bedoop sensor to get purchase credit in a tally maintained by the sandwich shop's computer.

Food stamps, health insurance cards, and written medical prescriptions, can likewise be encoded with digital data to enable the provision of new functionality.

At large trade shows, such as COMDEX, vendors needn't publish thick, glossy brochures to hand out to visitors. Instead, they may print various stylish promo cards for distribution. When later presented to a Bedoop sensor, each card leads to a web-based presentation – optionally including persuasive video and other multi-media components. The user can be prompted to provide data to customize, or focus, the presentation to the user's particular requirements. If the user wants further information, a request can be made by the click of a mouse (or the twist of a card).

Prizes and Product Promotions

Product packaging (e.g., Coke cans, Snapple bottles, Pepsi 12-pack boxes) can be encoded for contest purposes. The encoding can be customized, item to item, so that selected items – when Bedoop scanned – are recognized to be the one in a hundred that entitles the owner to a cash or merchandise prize. A remote server to which the item's Bedoop data is provided queries the user for contact information (e.g., address, phone number) so the prize can be awarded or, for smaller prizes, the system can print out an award certificate redeemable at local merchants for products or cash. Once a winning item is identified to the remote server, its UID on the server is marked as redeemed so that the item cannot later be presented to win another prize.

In other such embodiments, all of the items are encoded identically. Winners are determined randomly. For example, during a contest period, persons around the world may present Coke cans to Bedoop systems. The corresponding Bedoop application on each user computer submits Bedoop data to a corresponding web address. The user's e-mail address may also be included with the submission. As this data is relayed to the corresponding server computer(s), every N^{th} set of data is deemed to be a winner, and a corresponding award notification or prize is dispatched to the Bedoop system from which the winning set of data originated.

The server computer that receives such contest submittals from client Bedoop systems can be arranged to prevent a single user from bombarding the server with multiple sets of data in an attempt to win by brute force. (This may be done, for example, by checking the included e-mail address or received IP address, and not considering a data submittal if the same address was encountered in data submitted within the past hour. Similar anti-brute-force protection can be provided on the user's computer, preventing, e.g., repeated contest data to be sent more frequently than once per hour. More sophisticated anti-brute-force measures can of course be provided.)

Non-planar product packaging, such as cylindrical soda cans, present certain optical issues in encoding and decoding which are detailed further below.

Product Information and Ordering

Product packaging and product advertisements can be encoded with Bedoop data that, when presented to a Bedoop system, initiates a link to a web page from which that product can be purchased, or more information obtained. Once the link has been established, the user can be instructed to manipulate the object in different of the earlier-described modes to effect different functions, e.g., move towards camera to order the product; move away from camera for product information. If the object is moved towards the camera to effect an order, the user can be prompted to further manipulate the object to specify delivery options (e.g., rotate left for overnight mail, rotate right for regular mail). If the object is moved away from the camera to request product information, the user can be promoted to further manipulate the object to specify the type of information desired (e.g., rotate left for recipes, rotate right for FDA

nutritional information, move up for information on other products in this family, move down to send an email to the product manufacturer).

Credit card or other customer billing information, together with mailing address information, can be stored in a profile on the Bedoop system, and relayed to the transactional web site either automatically when a purchase action is invoked, or after the user affirms that such information should be sent (which affirmation may be signaled by manipulation of the packaging or advertisement in one of the earlier-described modes). Other modes of payment can naturally be employed.

Computer Access Cards

This disclosure earlier considered access cards used to gain access to secure buildings. Related principles can be used in conjunction with computer access.

A driver's license, employee photo ID, or other such document can be presented to a Bedoop sensor on a computer. The computer recognizes the user and can take various steps in response.

One response is to log onto a network. Another is to set load a user profile file by which the computer knows how to arrange the desktop in the user's preferred manner. By manipulating the Bedoop-encoded object, the user can further vary the environment (e.g., rotate left to launch standard business productivity applications and software development applications; rotate left to launch lunchtime diversions – stock update, recreational games, etc.)

Hotel rooms are increasingly providing computer services. By presenting a driver's license, a Bedoop-equipped computer in a hotel room can link to a remote site indicated by the Bedoop data, obtain preference data for that user, and launch applications on the hotel computer in an arrangement that mimics that user's familiar work computer environment.

Audio/Video Disks, Software, and Books

Bedoop data can be conveyed by indicia or texturing on the surfaces of CD and DVD disks, on the labels (or authenticity certificates) or inserts or artwork for same, on the enclosures for same (e.g., jewel box, plastic case, etc.), on book dust jackets, on book pages, etc. Any of these objects can be presented to a Bedoop device to establish a link to a related web site. The consumer can then manipulate the object (or otherwise choose) to select different options.

For music, one option is to receive MP3 or other clips of songs by the same artist on other CDs, or of songs from other artists of the same genre. Another is to view music video clips featuring the same artist. Still another is to order tickets to upcoming concerts by that artist. In-store kiosks can permit tentative customers to listen to sample tracks before they buy.

Similar options can be presented for video DVDs. In the case of video, this can include listings of other movies with the same director, with the same star(s), etc. In the case of software, the options can include advisories, bug fixes, product updates and upgrades, etc. Naturally, the user can make purchases

from these sites, e.g., of other music by the same artist, other videos with the same star, software upgrades, etc.

Similar options can be accessed using Bedoop data associated with printed book materials.

Children learn the mechanics of turning book pages at an early age. Children learn to look at pictures on the pages of a book and they enjoy hearing the story that is related to the images. Generally, adults read the words and the child follows along looking at the pictures. Children enjoy repeatedly hearing the words of a story. The association of seeing pictures and repeatedly hearing the words is an excellent mechanism for learning to read and learning to enjoy books.

Embedded digital watermark data can automate the above process so that a child can see the pictures, and hear the words independently. Such an arrangement provides enjoyment for the child while teaching reading and love for books, and at the same time giving the child independence and familiarity with an automated mechanism.

More particularly, images in the book, or the paper substrates of the pages, contain digital watermarks. As a child turns the pages of the book, a camera captures the image and an associated computer reads the watermark. The watermark is then used to index a data store – either local or remote – to obtain text corresponding to the page being viewed. A text-to-speech converter is then employed to voice the text to the child. (Alternatively, the data store can contain digitized speech, rather than simple text – permitting different story characters to be given different voices, etc.) Thus, as a child turns the pages of the book, the child hears the words that are printed on the page. By turning pages, the child controls the process. The child will naturally make an association between the printed words and the words that are played by the computer.

Ad Tracking

Advertisers commonly use different advertisements for the same product or service, and employ means to track which ad is more effective within which demographic group. Bedoop can provide such functionality.

Consider a travel service web site that is promoting Hawaiian vacations. Bedoop data from several advertisements can lead consumers to the site.

Identical advertisements can be placed in several different magazines. Each is encoded with a different Bedoop UID. By monitoring the UIDs of the Bedoop inquiries to the site, the travel service can determine which magazines yield the highest consumer response (e.g., per thousand readers).

Likewise, within a single magazine, two or more advertisements may be encoded with Bedoop data leading to the site – again, each with a different UID. Again, analysis of the UIDs used in accessing the site can indicate which advertisement was the more effective.

The two UIDs in the foregoing examples may both lead to the same internet destination, or may lead to different destinations.

The instantaneous nature of the internet links permits advertisers to learn how consumer responses to print advertisements vary with time-of-day, yielding information that may assist in making ads for certain products more effective.

More elaborate variants and combinations of the foregoing are, of course, possible, If the consumers provide personal information in response to the ads (either by permitting access to pre-stored personal profile data, or by filling in web-based forms, or by manipulation of the ad (e.g., "please move the ad towards your Bedoop sensor if you drank coffee this morning")), still richer statistical data can be gleaned.

Rolodex of Cards

Bedoop-encoded business cards as detailed above can be accumulated and kept near the telephone or computer in a Rolodex-like arrangement. If a refrigerator ice-maker malfunctions, a homeowner can find the card for the appliance repairman used a few years ago, and present it to a Bedoop sensor. A link is established to the repairman's company (e.g., web site or via telephone). At a web site, the repairman may provide basic information, such as hours of availability, current fee schedule, etc. The homeowner may select an option (by card gesture or otherwise) to invoke a teleconference (e.g., NetMeeting) to consult about the problem. Or the homeowner may select another option to send e-mail. Still a further option may permit the homeowner to schedule a house call on the repairman's weekly calendar. Still a further option may permit the homeowner to view one or more short videos instructing customers how to fix certain common appliance problems.

Stored Value Cards

An electronic money system (e.g., of the sort detailed in US application 60/134,782, filed May 19, 1999) may encode Bedoop data on a card that leads to storage at which random-number tokens (which represent increments of money) are stored. Presenting the card to a Bedoop system launches an application that reads and encrypts the tokens and forwards the encrypted data to the clearinghouse computer of the corresponding bank to learn their remaining value. There the tokens are decrypted and checked for validity (but not redeemed). The bank computer responds to the Bedoop system, indicating the remaining value of the tokens on the card.

For security reasons, the storage containing the random-number tokens should not be generally accessible. Instead, the user must provide authentication data indicating authorization to gain access to that information. This authentication data may be a PIN code. Or the user may provide authentication by presenting a second Bedoop-encoded object, e.g., a driver's license to the Bedoop system. (Many other Bedoop systems may advantageously use, or require the use of, two or more Bedoop objects – either presented one after the other, or all at the same time. The Bedoop system can provide visual or audible prompts leading the user to present the further Bedoop object(s) as necessary.

Ski Lift Tickets

In accordance with another embodiment, ski lift tickets are Bedoop encoded to provide various functionality.

For example, instead of buying a lift ticket good for a day, a skier may purchase a ticket good for eight lifts. This data is encoded on the ticket, and sensed by a Bedoop sensor at each lift. The sensors are networked to a common server that tracks the number of lifts actually purchased, and updates the number as used. The skier is informed of the number of rides remaining on entering or leaving the lift. Statistical data can be collected about trail usage (e.g., N% percent of skiers ski all day along just two lifts, etc.).

Off the slopes, back at home, the used lift ticket may be presented to a Bedoop sensor to obtain current snow conditions and lift hours, or to review trail maps, or to order ski vacation packages. If the ticket is encoded with the owner's name, UID, or other information of commercial/marketing interest, local merchants may give the bearer discounts on selected goods in response to Bedoop scanning of the ticket and recovery of such information.

REI Membership Cards

Membership cards for certain stores can be Bedoop-encoded to provide added value to the member. For outdoor gear stores such as REI, presentation of the card to a Bedoop sensor can lead to a library of USGS maps, to web pages with current fishing and hunting regulations, etc. Naturally, the store's on-line ordering site is just a quick twist away.

Theme Park Tickets

Theme park tickets can be encoded with the age and gender of the visitor, and with additional data permitting the experience to be customized (e.g., from a roster of theme park personalities, the visitor's favorite is Indiana Jones). Throughout the park are kiosks to which the visitor can present the ticket to orchestrate the visit to follow a particular story line. Some kiosks issue premiums matching the age/gender of the recipient.

Car Keys

Car keys (or key ring fobs) are Bedoop encoded. When the car is taken to a shop for service, the mechanic presents the key to a Bedoop sensor, and thereby obtains the car's maintenance history from a remote server on which it is maintained. At home, the key can be presented to a Bedoop sensor and manipulated to navigate through a variety of automotive-related web sites.

In some embodiments, the Bedoop-encoded object is not used to navigate to a site, but is instead used to provide data once a user's computer is otherwise linked to a web site. A user surfing the web who ends up at a car valuation site can present a key to the Bedoop scanner. The Bedoop data is used to access

a remote database where the make, model, options, etc., of the car are stored. This data is provided to a database engine that returns to the user the estimated value of the car.

While visiting a mechanic's web site, presentation (and optionally manipulation) of a key or key ring fob can be employed to schedule a service appointment for the car.

Fashion Coordination

Some department stores and clothing retailers offer "personal shoppers" to perform various services. For example, a customer who is purchasing a dress may ask a personal shopper for assistance in selecting shoes or accessories that complement the dress.

A Bedoop-encoded garment tag on the dress can be employed to obtain similar assistance. In response to such a tag, a Bedoop system can query a database to obtain a mini-catalog of clothes and accessories that have previously been identified as complementing the dress identified by the tag. These items can be individually displayed on a screen associated with the system, or a virtual model wearing the dress - together with one or more of the recommended accessories - can be synthesized and depicted. The shopper may quickly review the look achieved by the model wearing the dress with various different pairs of shoes, etc., by repeatedly activating a user interface control (by mouse, touch screen, or garment tag gestures) to cycle through different combinations.

A shopper's credit card can be Bedoop-encoded so as to lead Bedoop systems of particular stores (i.e., stores pre-authorized by the shopper) to a profile on the shopper (e.g., containing size information, repeat purchase information, return history, style/color preferences, etc.).

Credit Card Purchases

When a consumer visits a commercial web site and wishes to purchase a displayed product, the transaction can be speeded simply by presenting a Bedoop-encoded credit card to a Bedoop sensor on the user's computer. The Bedoop data on the card leads to a database entry containing the credit card number and expiration date. The Bedoop application then sends this information (optionally after encrypting same) to the web site with instructions to purchase the depicted product.

(Impulse purchases are commonly deterred by the hurdles posed between the purchase impulse and the completed purchase. This and other Bedoop applications aid in reducing such hurdles.)

Product Marketing

Bedoop data relating to one product or service can be used to cross-market others products and services. Consider a consumer who purchases a pair of golf shoes. The box is Bedoop encoded. By presenting the box to a Bedoop system, the consumer is linked to a web page that presents various promotional offers. The consumer may, for example, elect to play a free round of golf at one or more identified local golf courses, or print a coupon for ten percent off any order of socks from an on-line sock

merchant. (Various means can be employed to prevent multiple redemptions from a single box. One is a serial number that is tracked by the web page or cross-marketed merchant, and only honored once. Another is identification data corresponding to the consumer that is tracked to prevent multiple redemptions.)

Product tags can likewise be Bedoop-encoded. A tag from an article of Nike apparel can lead to the Nike on-line store, where the user can buy more merchandise. If the tag is from a soccer jersey, a certain tag manipulation (e.g., rotate left) may lead the user to a special-interest soccer page, such as for the World Cup. A tag on a golf glove may lead to a website of a local golf course. Twist left to reserve a tee time; twist right to review course maps and statistics. Bedoop kiosks can be provided in retail stores to let consumers use the Bedoop features.

Travel Planning Services

After making a reservation at a resort, a consumer is typically mailed (by email or conventional mail) various confirmation information. If not already printed, the consumer can print this information (e.g., a confirmation card).

Bedoop-encoding on the printed object can lead to web-based information relating to the reservation (e.g., reservation number, the consumer's name, arrival/departure dates, etc.). If the consumer wishes to make dinner or golf reservations, this object is presented to a Bedoop system – either at the user's home, at an airport kiosk, etc. The system recognizes the object type and encoded data, and establishes a link to a remote computer that provides various information and scheduling services for the resort. By manipulating the object (or otherwise) the consumer selects desired dinner and golf tee times. The system already has the reservation number (indexed by the UID), so tedious provision of such data is avoided.

In some embodiments, the remote computer is not maintained by the resort, but is rather maintained by an independent travel service. (The travel service may also maintain the DNS leaf node server.) The computer can present a web page (branded by the travel service or not) that offers the scheduling options desired by the user, and also presents links to other information and services (e.g., offering entry tickets to nearby attractions, and advertising nearby restaurants).

Airline tickets (or e-ticket confirmations) can be similarly encoded with Bedoop data. These items may be presented to Bedoop systems – at a traveler's home or in airports – to permit review and changing of travel itinerary, reserve hotels and rental cars, secure first-class upgrades, check the airplane's seating arrangement, review frequent flier status, scan tourist information for the destination, etc.

Movie Tickets

As indicated earlier, movie tickets can be encoded with Bedoop data identifying, e.g., the movie title and date. When a movie viewer returns home, the ticket stub can be presented to a Bedoop system.

One of the options presented by the corresponding Bedoop application can be to launch a pay-per-view screening of the just-seen movie at a discounted rate. Another is to download the movie onto a writeable DVD disk at the viewer's home, perhaps serialized to permit playback only on that viewer's DVD player, or enabled for only a few playbacks, etc. (again, likely for a discounted fee). Still another option is to present web-delivered video clips from the movie. Another is to offer related merchandise for purchase, possibly at discount to retail. (These features may be available for only a limited period after the date encoded on the ticket stub.) Another is to alert the consumer to upcoming movies of the same genres, or with the same director or stars, or released by the same studio. Still another is to direct a web browser to an on-line ticket merchant for tickets to other movies. The consumer may navigate among these options by manipulating the ticket stub, or otherwise.

The same, or related, options can likewise be provided in response to Bedoop data detected from a book jacket presented to a Bedoop system.

Video Recording

A video recording device can be programmed to record a broadcast program by presenting a Bedoop sensor with a printed promotion for the program (e.g., an advertisement in a newspaper or TV Guide). Bedoop-encoded within the printed document is data by which the Bedoop system (which may be built into the video recorder or separate) can set the recording time, date, and channel.

Set Top Boxes

Many entertainment-related applications of Bedoop data can be implemented using television set top boxes. Such boxes include processors, and typically include a return channel to a control facility. The provision of a Bedoop chip and optical sensor can vastly increase the functionality these devices presently provide.

Special Event Tickets

Consider a ticket to a basketball game. By presenting the ticket to a Bedoop system, a user may access the web site of either team so as to review recent scores and statistics. The user may also obtain a web-based virtual tour of the arena, and review seating maps. The view of the playing field as seen from the user's seat location may be presented. Tickets for upcoming games may be ordered, as well as pay-per-view games and team souvenirs. For high-priced tickets, the user may be entitled to premium web features, such as on-line text-, audio-, or video-chat session with a team star on the day before the game.

Unlike conventional tickets, Bedoop-encoded tickets need not limit the user to a predetermined seat. While the ticket may be printed with a nominal seat, the user may present the ticket to a Bedoop sensor and access a web site at which a different seat can be reserved. On attending the event, the consumer presents the ticket to a Bedoop sensor that reads the ticket UID and looks up the seat assignment

most-recently picked by the consumer. It then prints a chit entitling the consumer to take the seat earlier selected from the transactional web site.

Signet Rings

Signet rings have historically been used to indicate a person's identity or office. Such rings, or other items of personal jewelry, can be encoded with Bedoop data (either by texturing or printing) and presented as necessary to Bedoop systems. The extracted Bedoop data can lead to a secure web site indicating the person's name and other information (i.e., a web site that has anti-hacking measures to prevent illicit change of the stored identification information). Such a signet ring can be presented to Bedoop systems that require a high-confidence confirmation of identity/authorization before proceeding with a Bedoop function.

I. Tattoos

Temporary tattoos are well known and typically include an ink or printed film that is transferred to a wearer's skin through some application process (e.g., wetting or otherwise). The artwork on the tattoo can be arranged to steganographically encode Bedoop data, facilitating machine recognition of the persons (or objects) tattooed. Youths can compile a contacts database simply by snapping digital photos of friends using an imaging-capable personal digital assistant. Such a computer device can decode the watermark, access a corresponding web dossier of information on the person photographed, and add such information to a contacts database.

E-Paper

While it is doubtless evident that a great variety of printing technologies can be employed in Bedoop applications, it should be noted that e-paper can be employed as well. E-paper, developed by Nicholas K. Sheridon of Xerox, and mass produced by 3M, is a thin layer of transparent plastic in which millions of small beads, somewhat like toner particles, are dispersed. The beads, each contained in a fluid-filled cavity, are free to rotate within those cavities. The beads are "bichromal," with hemispheres of contrasting color (e.g. black and white). Under the influence of a voltage applied to the surface of the sheet, the beads rotate to present one colored side or the other to the viewer. A pattern of voltages can be applied to the surface in a bit-wise fashion to create images such as text and pictures. The image persists until new voltage patterns are applied to create new images. The reader is presumed familiar with the US patents issued to Sheridon on this technology.

It will further be recognized that epaper can be used to convey digital data according to essentially any known watermarking method, and is also suitable for conveying digital information in data glyph form.

Post-It® Notes

Pads of Post-It® notes, or other pads of paper, can be marked by the manufacturer (either by texturing, watermarked tinting, ink-jet spattering, etc.) to convey steganographic data (e.g., Bedoop data). When such a note is presented to a Bedoop system, the system may launch an application that stores a snapshot of the note. More particularly, the application may mask the note-portion of the image data from the other image data, virtually re-map it to a rectangular format of standardized pixel dimensions, JPEG-compress the resulting image, and store it in a particular computer subdirectory with a name indicating the date of image acquisition, together with the color and/or size of the note. (These latter two data may be indicated by data included in the Bedoop payload.) If the color of the note is indicated by digital data (e.g., in the file name), then the image itself may be stored in grey-scale. When later recalled for display, the white image background can be flooded with color in accordance with the digital color data.

The Bedoop system may buffer several past frames of image data. When the object is recognized as a Post-It note whose image is to be saved, the system may analyze several such frames to identify the one best-suited for storage (e.g., check the spatial frequency content of the note as imaged in each frame, to identify the one with the finest detail), and store that one.

When a Post-It note is recognized by the Bedoop system, the system may emit a confirmation tone (or other response) to indicate that the object has been recognized, but not immediately execute the snapshot operation. Instead, the system may await a further instruction (e.g., gesture) to indicate what operation is desired.

By moving the note towards the sensor, for example, the user can signal that a snapshot operation is to be performed. (This closer presentation of the note may also permit the imaging system to capture a more detailed frame of image data.)

By moving the note away, the system may respond by reading, decompressing, and displaying the six most-recently stored Post-It note images, in tiled fashion, on the computer screen. The individual notes can be displayed at their original dimensions, or each can be re-sized to fill the full height or width of a tile. A user interface control (responsive to gestures, mouse operation, keyboard scroll arrows, etc.) allows the user to scroll back in time to any desired date.

The full 64-bit Bedoop payload of other embodiments may not be needed for Post-It notes. In the just-given example, for example, the Bedoop system responds to all Post-It notes in the same fashion. Thus, an abbreviated Bedoop format that indicates simply 'I'm a Post-It note, yellow, size 3" x 3"' can suffice. The twelve bit CLASS ID, with eight further bits to indicate color/size combinations, may be sufficient. Reducing the payload permits it to be more robustly encoded on small objects. (As noted below, Bedoop decoding systems can look for several different data formats/protocols in trying to extract Bedoop data from an object.)

Alignment of Documents for Other Purposes

While the just-described pre-marked paper triggered a Bedoop response when presented to a Bedoop sensor (i.e., take a snapshot of the paper), the markings can be used for purposes other than to trigger Bedoop responses.

Regardless of the particular data with which the paper is encoded, the embedded subliminal graticules, or other steganographically-encoded registration data, can be used by other applications to correct misalignment of scanned data. In a photocopier, for example, a document need not be placed exactly squarely on the glass platen in order to yield a properly-aligned photocopy. The scanner scans the skewed document and then detects the steganographic registration markings in the resulting scan data. This data is then processed to virtually re-register same, so that the registration markings are in a desired alignment. The processed scan data is then provided to the xerographic reproduction unit to yield a photocopy in which the skew effect is removed.

The same technique is likewise applicable to video recorders, digital cameras, etc. If such a device images an object (e.g., a photograph) with steganographic registration markings, these markings can be used as a guide in re-registering the resulting data to remove mis-alignment effects.

Postal Mail Information

Many contexts arise in which data to be presented to a consumer is valuable only if timely. The postal service mail is ill-suited for some such information due to the latency between printing a document, and its ultimate delivery to a recipient. Bedoop principles, however, allow the recipient to take a postal object that was printed well before delivery, and use it on receipt (i.e., present to a Bedoop system) to receive up-to-the-minute information. In this and other embodiments, the Bedoop data can also uniquely identify the addressee/recipient/user, so the web site can present data customized to that user.

Distributors of printed advertising can reward Bedoop-driven consumer visits to their web sites by issuing digital tokens or coupons that can be redeemed for premiums, cash-back, etc. Every millionth visitor wins a million pennies (with appropriate safeguards, e.g., preventing more than one entry an hour).

Classes of Bedoop Encoding

The above-described embodiments focused on use of Bedoop data after decoding. Additional insight may be gained by examining the earlier part of the process – encoding.

Encoding can be performed in many contexts, which may be conceptualized as falling into three broad classes. The first is static marking, in which a document designer, pre-press service bureau, advertising agency or the like embeds Bedoop data. The second is dynamic marking, in which automated systems encode, or vary, Bedoop data "on the fly." Such systems can tailor the Bedoop data to particularly suit the context, e.g., to the moment, place, user, etc. The third is consumer marking, in which Bedoop data is added to a document at the time of printing.

The second class of encoding enables features not available from the first. Consider an American Express travel web page with information about travel to Hawaii. A DNS leaf node server points to this page in response to certain Bedoop data – e.g., data encoded in a magazine photograph of a Hawaiian beach scene.

Actually, all Bedoop data having a certain CLASS and DNS ID may lead to this web page, irrespective of the UID data. If the magazine photo is encoded with a particular "don't care" UID field (e.g., 111111111111111111111111), this may signal the originating Bedoop system – or any intervening system through which the Bedoop data passes – that arbitrary data can be inserted in the UID field of that Bedoop packet. The originating Bedoop system, for example, can insert a dynamically-configured series of bits into this field. Some of these bits can provide a profile of the user to the remote server, so that the Bedoop response can be customized to the user. (The user would naturally pre-approve information for such use so as to allay privacy concerns.)

As one example, the local Bedoop system can set the least significant bit of the UID field to a "0" if the user is male, or to a "1" if the user is female. The next four bits can indicate the user's age by one of sixteen age ranges (e.g., 3 or less, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15, 16-17, 18-20, 21-24, etc.).

Alternatively, or in addition, the local Bedoop system can stuff the don't-care UID field (all of it, or in part) with signature data tending to uniquely identify the local Bedoop system (e.g., system serial number, a hash code based on unchanging data unique to that system, etc.) By reference to such data, the remote server can identify repeat visits by the same user, and can tailor its responses accordingly (e.g., by recalling a profile of information earlier entered by the user and stored at the remote server, avoiding the need for data re-entry).

More on Optical Input Devices

It is expected that image input devices will soon become commonplace. The provision of digital cameras as built-in components of certain computers (e.g., the Sony Vaio laptops) is just one manifestation of this trend. Another is camera-on-a-chip systems, as typified by U.S. Patent 5,841,126 and detailed in Nixon et al., "256x256 CMOS Active Pixel Sensor Camera-on-a-Chip," IEEE J. Solid-State Circuits, Vol. 31(12), pp. 2046-2051 (1996), and Fossum, "CMOS Image Sensors: Electronic Camera-on-a-Chip," IEEE Transactions of Electron Devices, vol. 44, No. 10, Oct. 1997. Still another is head-mounted cameras (as are presently used in some computer-augmented vision systems). These and other image input devices are all suitable for use in Bedoop systems.

Camera-on-a-chip systems can be equipped with Bedoop detector hardware integrated on the same chip substrate. This hardware can be arranged to find and decode Bedoop data from the image data – notwithstanding scale, rotation, differential scaling, etc. Gestural decoding can also be provided in hardware, with the resulting data output in packet form on a serial output bus. Such a chip can thus

provide several outputs – image data (either in raw pixel form, or in a data stream representing the image in one of various image formats), 64 bits of Bedoop data (serially or in parallel), and decoded gesture data.

In other embodiments, the Bedoop detector (and/or the gestural decoder) can be on a substrate separate from the camera system.

To accommodate different Bedoop data formats and protocols, the hardware can include RAM or ROM in which different format/protocol information is stored. (These different formats/protocols can relate, e.g., to Bedoop systems employing different data payload lengths, different subliminal grids, different encoding techniques, etc.) As the Bedoop system stares out and grabs/analyzes frames, each frame can be analyzed in accordance with several different formats/protocols to try and find a format/protocol that yields valid Bedoop output data.

Movable Bedoop Sensors

Although the illustrated Bedoop systems are generally stationary, they need not be so. They can be portable. Some such systems, for example, employ palmtop computers equipped with optical sensor arrays. If the palmtop is provided with live network connectivity (e.g., by wireless), then Bedoop applications that rely on remote computers can be implemented just as described. If the palmtop is not equipped with live network connectivity, any Bedoop applications that rely on remote computers can simply queue such communications, and dispatch same when the palmtop next has remote access (e.g., when the palmtop is next placed in its recharger and is coupled to a modem through which internet access can be established).

Another variant is a Bedoop sensor with a 1D or 2D photosensor array (e.g., CCD or CMOS) that is movable around a desk or other work-surface, like a mouse. Such a sensor can be coupled to the associated computer by cabling, or a wireless interface can be used. The peripheral may be arranged for placement on top of an item in order to read digital data with which the object is marked. (Built-in illumination may be needed, since the device would likely shadow the encoding.) Some forms of such peripherals are adapted to serve both as general purpose digital cameras, and also as Bedoop sensors.

Such a peripheral would find many applications. In "reading" a magazine or book, for example, it may be more intuitive to place a Bedoop reader "on" the object being read, rather than holding the object in the air, in front of a Bedoop sensor. This is particularly useful, e.g., when a magazine page or the like may have several differently-encoded Bedoop sections (corresponding to different articles, advertisements, etc.), and the user wants to assure that the desired Bedoop-encoded section is read.

The "bookmark" paradigm of internet browsers might be supplemented with paper bookmarks, e.g., Bedoop data encoded on one or more pages of paper. To direct a browser to a particular bookmarked destination, the peripheral is simply placed on top of the page (or part thereof) that is marked with the corresponding Bedoop data. A user may print a "map" comprised of postage stamp-sized regions tiled together, each of which regions represents a favorite web destination.

Such a map may be printed on a mouse pad. Indeed, mouse pads with certain maps pre-encoded thereon may be suitable as promotional materials. A company may offer to print a family photograph on such a pad. Encoded within the photograph or the pad texture are addresses of web sites that have paid a fee to be accessible in this manner on a user's desk.

In this and other contexts, it will be recognized that the gestural input concepts detailed earlier involve relative movement between the sensor and the encoded object. In most of the earlier examples, the sensor is stationary, so gesticulation is effected by moving the object. Naturally, if the sensor is moveable (e.g., as a mouse or cell phone), the gestural movement can be effected by moving the sensor instead.

One particular embodiment of the arrangement detailed above a modified version of the Microsoft IntelliMouse with IntelliEye technology. That device includes a multi-element optical sensor integrated on an IC with various detector and processing circuitry, operating in conjunction with a short focal length imaging lens and an LED illumination source (all available from Agilent, as detailed below). The circuitry tracks movement of patterns across the sensor's field of view, by which the mouse's movement can be deduced. The Microsoft product collects 1500 data sets per second – a frame rate much higher than is generally needed for the present applications. Some such embodiments combine the functionality of a mouse with that of a Bedoop image sensor.

Such a mouse-like peripheral can omit the buttons and position-sensing features commonly provided on traditional mice, yielding a simple desk-facing palm camera that generates frames of data corresponding to a small area under the sensor portion of the mouse. More typically, however, the peripheral includes the buttons, roller wheels, and/or X-/Y- position sensing arrangements of traditional mice so that button and positional forms of data input can be exploited in interacting with the Bedoop application.

The optical data collected by the sensor can be processed within the peripheral's processor to extract the steganographically encoded binary Bedoop data therefrom. Or this processing burden can be undertaken by the associated computer system, with the peripheral simply processing and formatting the raw sensor data into sequential frames of image data to be output to that system.

While scanning peripherals of the type described above are typically wired to an associated host system, wireless links (e.g., radio, infrared, ultrasonic, etc.) can of course be used, freeing the user from the constraint imposed by the cable.

Hand Scanners – More

To elaborate on the concepts introduced above, the following paragraphs particularly detail a hand scanner modeled after the Hewlett-Packard CapShare 920. The scanner may be configured for use with any type of identifier, e.g., watermark, barcode, OCR, etc.

The reader is presumed familiar with the workings of the HP CapShare scanner. Such information has been published in the technical literature, e.g., Allen, Ross R. et al, "Processes for

Freehand Image Capture: HP CapShare Technology," The Society for Imaging Science & Technology PICS Conference, pp. 43-46, March 26, 2000. The CapShare scanner employs an optical sensor tracking engine assembly, comprised of part Nos. HDNS2000 (IC sensor chip), HDNS-2100 (lens with light pipe), HDNS-2200 (LED clip), and HLMP-ED80 (639 nm LED), the use of which is detailed in Agilent Application Note 1179, all available from Agilent Technologies, Palo Alto, CA.

As shown in Fig. 13, the CapShare scanner 210 functionally includes a CPU 212, a memory 214, a linear CCD array 216, first and second 2D CCD arrays 218a, 218b, a user interface (including an LCD screen and associated buttons) 220, and an interface 222 (e.g., a serial port and an IRDA port/transceiver) to an auxiliary device 224. Although not particularly shown, each of the CCD sensors has an associated LED system for illuminating the object being imaged.

A further enhancement to the CapShare scanner is to provide a wireless internet interface for interface 222, permitting direct communication between the device 210 and the internet.

The linear sensor 216 operates in a conventional manner, acquiring successive pixilated line-scans of imagery under the scanner at a pixel data rate of about 18 Mbits/second (permitting full accuracy scanning even at instantaneous scanner motion speeds of up to 16 inches per second).

The two 2D CCDs 218a, 218b, are spaced apart, adjacent the linear sensor, and are used to track the scanner's movement. The areas scanned by these CCDs are illuminated obliquely by IR light, highlighting microscopic media surface features. The CPU identifies patterns in the surface features detected by each of these CCDs, and tracks their movement from one frame to the next to discern the movement of the two CCDs. By knowing the movement of the two CCDs, the movement of the scanner itself can be determined. This scanner motion information is used to re-map the swathed scan data acquired from the linear scanner array into composite pixel data with uniform scanline spacing. This remapped data is the final scan data that is typically provided to the end user or application.

The sizing of the linear and 2D CCD arrays is left to the designer. If 600 dpi line scan resolution is desired across a four inch scan swath, a 2400 element linear CCD would be used. The 2D CCDs are typically smaller in extent, e.g., having an aperture of 0.25 inches x 0.25 inches. The spacing of the CCD elements is selected based on the size of surface features to be tracked.

The memory 214 includes both RAM and ROM. The RAM is used both for raw data storage, and for storage of final results. The scanner's operating system, pattern matching and data processing algorithms, and other program code are stored in the ROM.

In accordance with the illustrated embodiment, the ROM code also includes instructions for examining the final-result scan data (i.e., after re-mapping) for watermark data. In one particular embodiment, this is a two-step process. The final-result data is first screened by the CPU to determine whether it has certain hallmarks associated with watermarked data (e.g., the presence of a calibration signal, as detailed in U.S. patent 5,862,260). If such hallmarks are found, a more computationally-intense watermark decoding algorithm is performed. By checking for watermark information in such a two-step

process, CPU time isn't spent needlessly trying to extract a watermark from image data that apparently has no watermark.

In some embodiments, the watermark processing operation(s) occurs without user intervention – each time the raw scan data is processed and remapped into final-result form. In other embodiments, the watermark processing is invoked in response to a user command entered through the user interface 220. In still other embodiments, the watermark processing is invoked in response to a command provided to the scanner from an associated auxiliary device 224 (e.g., a local personal computer, a remote server computer, a specialized internet appliance, etc.).

In some embodiments, the decoded watermark payload data is transferred to an associated auxiliary device whenever such data is detected. In other embodiments, the data is not sent unless the auxiliary device 224 first asks for it. Such an auxiliary device request may be made by a software program that is executing on the auxiliary device, e.g., through an API call.

A watermark decoded by the scanner can be presented to the user on the scanner's LCD display 220. Or the scanner can forward the decoded watermark to a remote device 224, which can then reply with supplemental data for presentation to the user, as detailed elsewhere in this specification.

In some embodiments, the information obtained by the 2D CCDs 218a and/or 218b can be used to augment the information provided to the CPU so as to aid in the watermark detection/decoding process. For example, the 2D sensors provide 2D information immediately – without the time delay associated with remapping the 1D data from the linear CCD array into final form. This immediate 2D information may be analyzed for the presence of a calibration signal – perhaps shortening or obviating analysis for the calibration signal in the final data.

The 2D data can also be used to characterize the texture of the imaged substrate. Knowing the substrate texture allows the CPU to apply filtering or other watermark-enhancing/image enhancing steps as best fits the particular circumstance.

The 2D data also allows the CPU to assess the relative quality of different regions of line-scan data in the final scan data. In Fig. 14, an object 230 is scanned by a scanner 210 traveling an arced path, yielding successive lines of raw scan data 228. The geometry of the arc is revealed by data collected by the two 2D CCDs (which serve as motion encoders). Where the successive lines are spaced closer together (as at region A), the raw scan data is of higher resolution (relatively "oversampled"). In contrast, where the successive lines are spaced further apart (as at region B), the raw scan data is of lower resolution (relatively "undersampled"). In its screening or analysis for subtle watermark data, the CPU can be instructed to look first in region A, reasoning that the higher quality of the raw data in this region is most likely to include usable watermark information. (In some embodiments, watermark screening and/or detection may proceed by reference to the raw scan line data, rather than waiting for the data to be remapped into final form.)

The two CCDs 218a, 218b also permit various binocular processing to be performed so as to enhance, or allow for more intelligent processing, of the linear scan data. Consider, for example, the case where the image being scanned doesn't convey a perfectly planar (e.g., rectilinear) signal. The substrate could be warped, or the image may have been printed in a skewed manner, or some other transformation may have taken place that creates an image that changes orientation/scale over its extent. One such example is shown in Fig. 15, which depicts a watermark calibration signal (here presented as an overt grid, for clarity of illustration). Each of the two 2D CCDs 218a, 218b senses a differently-oriented calibration signal. By reference to differences in the data sensed by the two spaced-apart CCDs, the CPU can infer scale, rotation, or other image transformation at intermediate points, and apply a compensation to the scan data so as to counteract such distortion.

Such compensation need not be based on a watermark calibration signal. Any other optically-sensed attribute at the two spaced-apart points may be used to infer the same, or related attributes, at intermediate positions, permitting appropriate compensation(s) to be applied.

Another application of the spaced-apart sensors 218 is to bi-optically determine the distance from the scanner to the object being imaged. Consider Fig. 16, which shows a scanner 10 with two spaced-apart CCD sensors 218a, 218b, imaging a warped object 232 (e.g., a warped paper substrate, or a curved object such as a drink can). In the depicted example, the first CCD 218a detects a very crisp image of surface texture or imagery, whereas the second CCD 218b detects an image similar to the first CCD, but blurred – as if low-pass filtered. Software instructions for CPU 212 can cause the scanner to recognize that the part of the object 232 under CCD 218a is immediately adjacent the scanner (and adjacent the nearby portion of the linear CCD array 216), whereas the part of the object under CCD 218b is spaced somewhat from the scanner.

Having information about the spacing of the object 232 from different parts of the linear sensor array permits certain compensations to be made in the data collected by the linear scanner. In the case of watermark detection, the CPU may recognize that data from the end of the linear scanner 216 remote from the object 232 will be devoid of meaningful high frequency information. In many watermark detection algorithms, the CPU can disregard data from such portion of the linear scanner – allowing it to focus on portions of the image data with the necessary high frequency components, thus producing more reliable results more quickly.

In other watermarking systems, two watermarks may be present – one conveyed in reliance on high frequency image components, and another encoded mostly with low frequency image components (i.e., in anticipation of circumstances where the object is imaged slightly out-of-focus). Upon recognizing that the linear scan data is weak in high frequency components, the CPU can be programmed to look just for the low frequency watermark data.

Just as the scanner 210 can perform watermark decoding, it can similarly perform barcode decoding. Conventional pattern-recognition algorithms can be applied by CPU 212 to either the raw or

final scan data to identify barcode patterns. Once the pattern is identified, decoding is straightforward by applying known barcode alphabets. As in the watermark case, barcode decoding can be performed autonomously, or in response to user/auxiliary device command. Similarly, the decoded barcode data can be provided to the auxiliary device whenever detected, or in response to an auxiliary device query. The 2D data can likewise be used to augment the information provided to the CPU so as to aid in the barcode detection/decoding process.

In similar fashion, the above-described benefits associated by use of the two 2D CCDs can similarly be applied in the barcode context.

As earlier described, once the identifier information is extracted from the image data, internet links can be based thereon to provide supplemental information, e-commerce opportunities, etc. In many implementations, the scanner UI 220 is used to present this supplemental information to the user, e.g. by software instructions that render HTML instructions for presentation on the UI display screen. The UI controls (e.g., buttons) can likewise be used to receive user instructions and commands, for linking back to the internet.

Cell Phones as Bedoop Devices; GPS Receivers

Bedoop technology can be integrated into portable telecommunication terminals, such as cell phones (manufactured, e.g., by Motorola, Nokia, Qualcomm, and others). Such a phone can be equipped with a 1D or 2D image sensor, the output of which is applied to Bedoop decoding circuitry within the phone. This decoding circuitry can be the phone's main CPU, or can be a processing circuit dedicated to Bedoop functionality. (In this as in other embodiments, , the decoding can be effected by dedicated hardware, by decoding software executing on a general purpose CPU, etc.)

Cell phones are already equipped with numerous features that make them well suited for Bedoop operation. One is that cell phones typically include an LCD or similar screen for display of textual or graphic information, and additionally include buttons or other controls for selecting among menu options presented on the screen (e.g., by moving a cursor). Moreover, cell phones naturally include both audio input and output devices (i.e., microphone and speaker). Still further, the protocol by which cell phones transmit data includes data identifying the phone, so that such data need not be separately encoded. And finally, cell phones obviously provide ready links to remote computer systems. Collectively, these capabilities rival those of the most fully-equipped desktop computer system. Thus, essentially all of the applications detailed elsewhere in this specification can be implemented using cell phone Bedoop systems.

As with the other Bedoop systems, when Bedoop data is sensed, the phone can respond to the data locally, or it can forward same over the cellular network to a remote system (or computer network) for handling.

One application that may be invoked locally (i.e., within the phone) is the dialing of a corresponding telephone number. In some embodiments, the phone number is literally encoded as part of

the Bedoop data payload. In others, the phone number is stored in a memory within the phone, and indexed in accordance with an identifier decoded from the Bedoop data.

The variety of operations that can be handled remotely is virtually limitless. Some entail interaction with the user. For example, the remote system may initially respond by presenting to the user a menu of options on the display screen (e.g., Purchase, Add to Shopping List, Request Sample, Add to Notepad, etc.) The user then responds by providing further input (e.g., by manipulating one or more buttons on the phone, by providing spoken instructions to a voice recognition sub-system within the phone, etc.). This further data is then dispatched from the phone, and the requested action undertaken. Other operations don't require further interaction with the user, but immediately invoke a corresponding action.

While the just-described arrangement included the Bedoop decoding function within the phone, in other embodiments the image data can be transmitted from the phone and decoded at a remote location.

Reference was earlier made to GPS receivers as permitting the location of a person to be tracked, and contact information updated accordingly. GPS receivers find many other applications in Bedoop contexts. For example, the response of a Bedoop system can be tailored, or vary, in accordance with the location of the person invoking the operation. To illustrate, if a user presents a newspaper insert or coupon for a Dominos pepperoni pizza meal to the Bedoop sensor on a GPS-equipped cellular phone, the GPS data can be encoded in the Bedoop data dispatched to the Domino's Bedoop server. That server can identify, by reference to the GPS data, the location of the nearest Domino's franchise, and can forward the order to that franchisee. The franchisee, in turn, can telephone the user (by reference to telephone number data from the cell phone) to confirm the order, inquire if additional items are desired, inform the user of the final price, and to obtain the delivery address. (The latter step can be omitted; the franchisee can employ the GPS data to obtain the corresponding street address, e.g., from map data licensed through NavTech of Chicago.)

The protocols by which the Bedoop data, GPS data, and cell phone identification data are conveyed from the phone to the cellular network can take various forms; the design of such systems are familiar to those in the relevant arts. In one embodiment, the protocols by which some cell phones are now provided with email or internet access are further adapted to convey Bedoop and GPS data. The protocols for conveying telephone identification data are already well established. Once received by the cellular network, the Bedoop data can be formatted into packets, either incorporating the GPS data and telephone data into the same packet structure, or by formatting such data into separate packets accompanying the Bedoop packets.

The provision of image sensors in cell phones enables other functionality. One is the capture of still or video imagery. Such image data can be compressed (typically by lossy processes such as MPEG, JPEG, or the like, implemented with dedicated hardware CODECs) and transmitted with the audio data. The screens on such phones can likewise be used for display of incoming image or video data.

Another function enabled by image sensors in cell phones is user-verification, e.g., by retinal scanning or other optically-sensed biometrics, before the phone will permit a call to be placed. A great number of such biometric verification techniques are known.

Cell phone Bedoop sensors may not always be in communication with the cell phone network. The phone may be out of range of a cell site, or may be in operational mode in which an RF link is not then established. In such events, any Bedoop data sensed by the phone that is to be handled remotely is desirably stored locally within the phone, and queued for transmission to the cellular network the next time communication is established (a so-called "store and forward" form of operation).

Catalog Advertising

Any form of hand-held scanner - whether of the type just described or others known in the art - offers a convenient way to interact with catalog advertising. Imagine a traditional paper catalog, e.g., from L.L. Bean, Inc., or Lands End. Each image in the catalog is Bedoop-encoded with a code that identifies the depicted product (and, if necessary, the manufacturer, etc.). A user browsing through the catalog, on seeing a product of interest, places the scanner over the picture (and optionally may be required to push a button or otherwise signal to initiate further processing). The scanner detects the Bedoop data and relays it to an associated computer (optionally with data identifying the consumer). The computer polls a remote server computer maintained by the merchant, which responds with data corresponding to the item depicted in the scanned image. This returned data can include data indicating the sizes available, data indicating the colors available, data indicating the variant styles available, flag bits indicating whether each item is in stock, etc. This returned data can be presented to the consumer – typically on a display device but alternatively in audible form.

Preferably, the customer's body measurements (waist size, inseam length, neck size, etc.) are stored in a user profile, either on the local computer, at the merchant's server computer, or at the computer of a third party service provider. This allows the system to customize the data presented to the user – e.g., showing the color options and availability only for the depicted shirt in a 16 inch neck and a 34 inch sleeve length.

If necessary, the user can select among the color or style options, using the handheld input device (either buttons, gestures, etc.), or any other input device. Or the item may be one for which no further specifications are needed. In either event, once the desired product has been sufficiently specified, the user can signal the system to place the order. Payment and shipping details can be arranged through any of the great variety of techniques known in the art, e.g., by charging to a credit card number and shipping to an address on-file with the merchant.

1. Revenue Sharing

When a consumer presents a Bedoop-encoded object to a sensor, and as a result of the link(s) thereby established, purchases a product or service, the revenue from that transaction may be shared with the participants who made it possible. In the case of a Bedoop-encoded magazine ad, some of the participants may include (1) the photographer or graphic designer who produced artwork used in the ad; (2) the advertising agency whose creative talent led to the ad; (3) the publisher of the magazine in which the consumer encountered the ad; (4) the service provider(s) who provided the transport channel(s) between the consumer and the vendor; and (5) the service provider who maintained the server that ultimately linked the Bedoop data to the vendor's web site.

Gambling Applications

Casinos around the world deploy considerable resources each year to deter cheating. To that end, playing cards and chips used for gaming and betting could be encoded with digital watermarks and used to enhance security. In order for the application to work, playing cards and chips would be encoded with data unique to each casino, game, card deck and/or face value. Then, cameras placed above gaming tables would be used to read the information off the cards and chips. The information from the cards could be used to alert security or keep records of suspicious activity in the following ways.

A camera placed above a card gaming table (like Blackjack) could read the data encoded in the backs of the cards determining the authenticity and face value of those cards. This means the camera could catch anyone trying to replace cards after they were dealt-either by flagging cards as not being part of the deck currently in use or by flagging them as being a different face value than those dealt to the player. If a player switches cards after they are dealt, the watermark reader in the camera can alert security of the fraudulent activity.

Additionally, the data encoded in the cards can be used to track the winner(s) at the table. If the dealer and the player are in collusion, that player may be dealt winning cards on a regular, predetermined basis (based on tricky shuffling by the dealer). By watching the pattern and face value of cards that are dealt, it can be determined if a player wins at a much higher than average rate. Again, security personnel can be alerted to suspicious activity.

Cameras placed above gaming tables where chips are used (certainly not limited to card games) can be programmed to watch for watermarks in chips. Any chip that does not include the appropriate watermark can signal that a chip might be counterfeit. In another situation, the face value of the chips can be determined as they are placed on the table such that any switching of the chips after play begins will be noted.

The foregoing principles are more generally applicable to monitoring and surveillance systems employing digital watermark technology to identify monitored objects.

PART II

As noted, the following disclosure focuses on one particular application – a system for linking print media to electronic content. It should be reiterated, however, that the technology is not so limited, and may more generally be viewed as a system for linking any object (physical or electronic) to a corresponding networked or local resource.

In accordance with an exemplary application of the below-detailed technology, digital watermarking is employed to convey a plural bit identifier within print media, such as magazine advertisements or articles, direct mail coupons or catalogs, bank- or credit-cards, and business cards. This identifier is read by software in a user's computing device and forwarded to a remote database. The remote database identifies a URL corresponding to the identifier, and provides the URL back to the user's computer – permitting a browser on the user's computer to display the URL-identified web page. That web page can provide additional information or services – more timely and/or more extensive than that provided by the print material. By such arrangement, more efficient internet navigation and access is provided to consumers, and more effective means for linking readers to e-commerce points of sale is provided to advertisers.

Before beginning a detailed exposition, it may be helpful to provide an overview of the larger system of which the present technology forms a part. As shown in Fig. 1, the larger system entails four basic processes – registering, embedding, detection and response.

Registering refers to the process of assigning an ID to an object, and associating that ID with a corresponding action or response. Additional steps can be included, such as logging the name and/or organization of the registrant, the name of the product, a description of the object and a context in which it is found (magazine, book, audio track, etc.), etc.

Embedding refers to the process of encoding of an object with a digital identifier (e.g., a watermark conveying a serial number in its payload).

Detection is the complementary operation to embedding, i.e., discerning a digital identifier from an object.

Response refers to the action taken based on the discerned identifier.

The middle two steps -- embedding and detection – can employ any of myriad well-known technologies, including 1D and 2D barcodes, magnetic ink character recognition (MICR), optical character recognition (OCR), optical mark recognition (OMR), radio frequency identification (RF/ID), data glyphs, organic transistors, magnetic stripe, metadata, file header information, UV/IR identifiers, and other machine-readable indicia and techniques for associating plural-bit digital data with an electronic or physical object. The detailed embodiment employs watermarking technology, although this is illustrative only.

Referring to Fig. 2, a system 10 according to the exemplary embodiment includes an originating device 12, a router/server 14, a product handler 16, a registration database 17, and one or more remote resources 18.

The originating device 12 can take many different forms, e.g., a cell phone, a personal digital assistant (e.g., a Palm Pilot), a personal computer, a barcode scanning system, etc. For expository convenience, the embodiment is described with reference to a personal computer for device 12.

Device 12 interacts with an object 20. The object can be electronic or not. Electronic objects 20 can include computer files, representations of audio, video, or still imagery (e.g., files or in streaming form), etc. Non-electronic objects can include physical objects such as newspapers, magazine pages, posters, product packaging, event tickets, credit cards, paper currency, etc. Non-electronic objects can also include sounds produced by loudspeakers.

When used with non-electronic objects, device 12 (Fig. 2) typically includes some form of sensor or transducer 22 to produce electronic signals or data corresponding to the object. Examples include CCD- or CMOS-based optical sensors (either as part of still- or video cameras, flatbed scanners, mice, or otherwise), microphones, barcode scanners, RF ID sensors, mag stripe readers, etc. In such cases, the sensor 22 may be coupled to associated interface electronics 24, which in turn may be coupled to device driver software 26, which in turn may be coupled to one or more application programs 28. Device driver software 26 serves as a software interface, communicating at a relatively high level with the application programs 28 (e.g., through API instructions whose content and format are standardized to facilitate application programming), and at a relatively low level with the interface electronics 24.

The detailed embodiment contemplates that the object 20 is a magazine advertisement encoded with a steganographic watermark conveying a plural bit object identifier. The watermark is hidden in the advertisement's image in a manner indiscernable to human observers, but detectable by computer analysis. That analysis is performed by a watermark detector 30.

Watermark detector 30 can be implemented in various different locations in the system of Fig. 1. Typically, the detector is implemented in the originating device 12, e.g., in the driver software 26, or in application software 28c that serves to link to external resources based on detected watermarks. But it may be implemented elsewhere, e.g., in hardware in the interface electronics 24, in an operating system associated with the device, or outside device 12 altogether. Some systems may have plural watermark detectors, implemented at different locations throughout the system.

In an illustrative system, the watermark detector is implemented in the device driver 26. Functionality of the detector is made available to the application program 28c through one or more APIs specific to watermark-related functions. One function is reading of the watermark data payload from the object 20.

The illustrated application 28c is a software program that serves to communicate the watermark data from the device 12 to the router/server 14 through one or more communications links 32 (e.g., the internet). Application 28c also receives information from the communication links 32 and presents same to the user (or otherwise uses same).

The router/server 14 is a high capacity computer including one or more CPUs, memory, disks, and I/O ports. As is familiar to artisans, the disks store operating system software and application programs, together with data, that are transferred to the memory as needed by the CPU. The router essentially serves as a middleman between the application 28c and the product handler 16. As detailed below, the router receives requests from the application, logs them in a transaction log 15, and passes them on to the appropriate product handler.

As more particularly detailed below, the handler 16 provides a response in accordance with the particular watermark payload. The response may be provided directly by the product handler to the device 12, or the handler may respond by communicating with a remote resource 18 (which may be, e.g., a data repository or service provider).

In the former case, the handler 16 may identify a URL corresponding to the watermark (using the database 17), and return the URL to the application 28c. Application 28c can then pass the URL to a web browser 28b in the device 12, and initiate a link to the internet site identified by the URL. Or the handler may have some locally stored data (e.g., audio or video, or software updates) and send it to the device 12 in response to the watermark.

In the latter case, the handler 16 does not respond directly to the device 12. Instead, the handler responds by communicating with a remote resource 18. The communication can be as simple as logging receipt of the watermark message in a remote repository. Or it can be to authenticate device 12 (or a user thereof) to a remote resource in anticipation of a further transaction (e.g., the communication can form part of an on-line licensing or digital rights management transaction). Or the communication can request the remote resource to provide data or a service back to device 12 or to another destination (e.g., to initiate an FTP file transfer, or to request that a song selection identified by the watermark be downloaded to a user's personal music library, or to update software installed on device 12).

In still other cases, hybrids of the two foregoing cases can be employed, e.g., handler 16 can send some data back to device 12, while also communicating with a remote resource 18.

In some cases, the response returned to the device 12 by handler 16 (or a remote resource 18) can serve to trigger some further action by the device 12. For example, the response returned to device 12 can include a WindowsMedia audio file, together with a request that the device 12 launch the WindowsMedia player installed on the device. (The launching of a browser pointed to a URL is another example of such triggering.)

The illustrated product handler 16 comprises essentially the same hardware elements as the router 14, e.g., CPU, memory, etc. Although Fig. 2 shows just one product handler, several product handlers can be included in the system – either co-located of geographically distributed. Different handlers can be dedicated to different functions (e.g., serving URLs, serving music, etc.) or to different watermark sources (e.g., one responds to watermarks found in audio, another responds to watermarks found in print advertising, etc.). Further specialization may also be desirable (e.g., one handler may

respond to advertising placed by Ford, another may respond to advertising placed by Chevrolet; or one handler may respond to advertising appearing in Wired magazine, another may respond to advertising appearing in Time magazine, etc.). In one particular implementation, the router 14 dispatches the incoming data to one of several handlers in accordance with (1) the vendor of the originating application 28c, and (2) the particular identity of the application 28c.

The following discussion focuses on the data exchanged between the application 28c, the router/server 14, the product handler 16, and the associated protocols, in one illustrative embodiment.

II.

III. Concept of Operation

When shown a watermarked image, the application 28c analyzes the image and extracts the embedded watermark payload (more particularly detailed below) from the image. The application sends some or all of this information in a message format to the router 14.

The router 14 decodes the received message, looking for vendor and product information. Based on this information, it passes the message to a corresponding product handler 16.

The product handler receives the message and attempts to match the detected watermark serial number to a registered watermark serial number earlier stored in the database 17. If a match is found, the product handler performs the desired action. As noted, typical actions include returning a URL for web redirection, serving up an HTML page for initial user navigation, initiating software downloads, etc. If a match is not found, the product handler returns an error code and message to the application 28c. If a match is found, but the corresponding action is unavailable, incomplete, inactive or invalid, the product handler returns an error code and message to the calling application.

A generalized view of the foregoing is provided in Fig. 4.

(Note that while the system may concentrate on a certain type of object 20, and a certain vendor's application 28c, the architecture is constructed to support accessing product handlers from other vendors and corresponding to other objects. This concept makes the system suitable as a clearinghouse for processing all machine-readable indicia on web-enabled devices.)

An exemplary detection and response cycle is illustrated below.

User	*Application*	*Router*	*Product Handler*
Shows object to sensor 22			
	Acquires watermark *Creates message packet* *Sends packet to product handler*		
		Receives message packet *Logs transaction* *Decodes packet* *Identifies product sending packet* *Passes packet to*	

		Product Handler corresponding to product	
			Logs received packet *Validates packet serial number* *If not found, returns error packet to application* *Else, returns packet with data/action back to application (e.g., URL)*
	Receives packet *If error, display error message* *Else, display data or perform the requested action (e.g., launch browser and link based on received URL)*		
Sees the data/action associated with the object (e.g., views web page)			

The present system generalizes this example to support any product from any vendor that is capable of sending a message via the Internet that complies with the expected request format (e.g., a product code, message type, and identifier) and receiving a message in a corresponding response format. One set of message formats suitable for use in such a system are described in more detail below.

Watermark Registration – the first step in the process

In order for the system to identify the response (e.g., a URL) that corresponds to an object identifier (e.g., a watermark), this data must first be associated within the database 17 in association with the watermark to which it corresponds. The watermark registration process captures some basic identification information used later to validate the incoming message, and identifies the associated information/action. In the illustrated example the identification information includes:

- ?? *Customer Account,*
- ?? *Object and associated attributes (name, description, expiration, etc.),*
- ?? *Action, and*
- ?? *Registered Serial Number (for registration updates)*

The Customer Account identifies the watermark registrant. In most cases, this is also the party to be billed for services. For validation and security reasons, the Customer Account is required to be a known, existing account. Account information, including the account's password, is maintained by an Account Management system.

The Object and associated attributes identifies the object to be watermarked. The object attributes typically include the name and description of the object and a list of accounts authorized to access the object's registration. These authorized "supporting" accounts are typically the ad agencies, pre-press houses, etc. involved in the watermark embedding process in the print advertising example contemplated herein.

The Action defines the response the customer desires when the watermark is detected. It varies by product, but in the illustrative embodiment involves the return of some additional information regarding the watermarked object. In the illustrative system, the action is return of a URL or HTML to be used to display a web page associated with the watermarked object. For other products, the desired response may be display of the object's owner & rights information, software/data downloads, delivery of streamed audio or video, presentation of an advertisement, initiation of object-based actions, etc.

The Registered Serial Number forms the last component of the registration. It is this assigned vendor and product-unique identifier that allows the system to acquire the specific information/action for the object in question.

A few key product Registration concepts -

Watermark Registration is a product-specific process –

To allow each of the products the freedom to upgrade their capabilities without impacting any other product function or schedule, the registration process is product-specific.

Watermark registration is web-enabled -

The exemplary registration is a web-enabled process that requests the basic identifying information from the object owner (publisher, ad agency, studio, etc.) and returns to the registrant a packet with a unique identifier to be embedded within the object. A watermark embedding application (i.e., software) uses this packet to embed the watermark type and serial number within the client's object. In the illustrative system, only one watermark may be embedded within a single object. In other embodiments, multiple watermarks may be embedded into a single object.

When a customer registers a watermark, the system associates the watermark serial number with the information provided by the customer during the registration process. The associated information may vary with different products. One set of associations, for the exemplary magazine advertisement objects, is shown in the following table:

Mandatory?	***Information***	***Comments***
Mandatory	*Customer*	*Typically, the publisher*
Mandatory	*Publication(s)*	*Magazine(s) containing the ad*
Mandatory	*Issue Date*	*First date of the magazine/publication period*
Optional	*Volume*	*Magazine/publication volume information*
Optional	*Region Code*	*Optional information for regional publications*
Optional	*Location Code*	*Location of the object within the publication (e.g., page and, optionally, finer location data)*

Mandatory	*Watermark Type*	*Watermarks may have varying type. The type defines how to interpret the Serial Number*
Mandatory	*Serial Number*	*Assigned watermark number*
Mandatory	*Object Name*	*Customer's name for the object*
Mandatory	*Object Description*	*Customer's textual description of the object*
Mandatory	*Object Type*	*Ad or Editorial (and in other systems: Direct Mailer Card, Product Packaging, Coupon, Catalog, Business Card, Credit Card, etc.)*
Optional	*Campaign*	*For ads and promotions, the campaign name*
Optional	*Object size*	*Stated in fractions of the page (full page, half, etc.)*
Mandatory	*Effective Date*	*Date on which the user will first be able to initiate any actions. For publications, typically this is the "on stand" date*
Mandatory	*Expiration date*	*Date/time when the watermark expires*
Mandatory	*Primary Action*	*Initially the URL used for redirection*
Mandatory	*Primary Effective*	*Date the Primary action becomes effective*
Mandatory	*Primary Expires*	*Date the Primary action expires*
Optional	*Default Action*	*Reserved for future use (e.g., backup to the Primary action)*
Optional	*Default Effective*	*Date the Default action becomes effective*
Optional	*Default Expires*	*Date the Default action expires*
Optional	*E-mail address*	*Used to automatically notify the Customer of problems with the registration/Action*
Mandatory	*Status*	*Incomplete, active, inactive*
Optional	*Problem Indicator*	*Bad URL, slow site, etc.*
Optional	*Supporting Accounts*	*This field and its sub-fields are repeated for each supporting account*
Optional	*User Fields (4)*	
Optional	*Text*	*User Field free text*
Optional	*Viewable by Others?*	*Y/N. N hides the field form any other accounts*

Table 1. Registration Database Elements

Watermark registrations expire -

For some products, watermarks are granted only for a limited period of time. For these watermarks, the Registration process employs an expiration date for the assigned serial number. When the system receives a message requesting action for a serial number that has expired, an error is returned. Registrants may extend their watermark serial number expirations by updating the expiration date. Expiration extensions may result in customer charges.

Watermark registration can be completed in one or more web sessions -

Registration can be a single or multi-step process. If the media owner has all of the required information at the start of the process, the system can provide a simple web-enabled method for requesting a watermark serial number (s) on-line. With all of the information provided, the registration is considered "active." That is, it is available for immediate use by the consumer. If the registrant does not have all of the required information available at the initial session, by providing a minimum set of information (e.g., name and/or organization name + product), a product watermark serial number may still be issued for the

registrant to use in the embedding process. The most typical use of this partial registration occurs when the actions associated with the media to be watermarked (e.g., URL, etc.) are not yet known. The partially registered serial number is considered "inactive" until all of the required registration information has been completed. The system will issue an error message if requested to process an "inactive" serial number. Whether active or inactive, these registrations may be considered billable items subject to the terms and conditions of the applicable contract(s).

Registrations can be updated by the customer to reflect new information and/or to complete a previous registration session. For example, a registered customer may request a watermark serial number without specifying the URL used to redirect the consumer. The system will assign a serial number so that the customer can continue with the embedding process, but the registration will not be considered complete until the customer updates the registration with the URL and any other mandatory information regarding this serial number.

Watermark registrations are secure -

Only the registrant and those accounts that the registrant authorizes can access specific watermark registrations.

In the illustrated system, the customer account that registers a watermark may grant permission to a specific ad agency and/or pre-press house to change certain fields within the registration as a normal part of their work. Each customer, agency and pre-press house needs an account on file to be granted access to watermark registrations. The Customer account is established as part of the contract process. For ad agencies and pre-press houses, the accounts are established on an as-needed basis, through a controlled web site accessible to the customer.

For all products, the same basic tenet holds – access to the registration information is limited to only explicitly authorized accounts. Accounts are password protected. For ad agencies and pre-press houses, a single password may be shared. In other embodiments, each part may be assigned a unique password.

Watermark registration changes are logged –

All registration actions – creation, modification and deletion - are logged in an audit log. The authenticated username, the date/time of the action, and the action itself are all stored to provide a complete audit trail.

Processes and data flows associated with registration are illustrated in Fig. 6.

Entering Data into the Registration Database

While the client application, router, and product handler have initially been described in connection with responding to watermark information sensed from media objects, the same infrastructure can be employed earlier in the process, to enter data into the registration database 17. That is, a suitably configured variant of application 28c can be used by publishers, ad agencies, pre-press houses, etc., to (a)

provide initial data to the database; (b) update such data; and (c) query the database for current values. Alternatively, a dedicated registration server 19 (Fig. 2) can be employed.

The involvement of plural parties in the registration process can be facilitated by encapsulating the database record contents for a given watermark in a file to which information is successively added (or updated) by different entities, and used to convey data between the database 17 and the cited entities.

Consider a case where Nike advertises in Wired magazine. The ad department at Wired agrees to sell space in response to a request from a media buyer at Nike. Wired may start the related watermark work by securing from the operator of system 10 a particular watermark identifier. (This, and most of the following procedures, are effected by computers talking to computers in accordance with instructions provided by suitable software used by the various participants, etc. In the discussion that follows, this software is the registration server 19 although, as noted, product handler 16 could be arranged to perform these functions.) Wired provides the operator an issue identifier (e.g., San Francisco edition of the July, 2000 issue), and internal tracking information used by the magazine. Registration server 19 responds by sending Wired a confirmatory file, by email, that encapsulates the information thus-far (i.e., the watermark identifier, the issue ID, and the magazine tracking information). Server 19 creates a new database record, and parses the received information into corresponding fields of the record.

Wired forwards the file received from the registration server to the media buyers at Nike. Nike supplements the information with its additional data, including the name of the advertisement and internal tracking information. It then forwards the updated file to server 19. Again, this server processes the file and updates the database record with the new information. It emails a confirmatory data file to both Nike and Wired, so each has the latest set of information.

The process continues in this fashion. Each entity provides new data to the registration server 19 via an emailed encapsulating file. The server updates the corresponding database record, and dispatches updated versions of the encapsulating file to the identified participants so each has the latest information.

Once Nike has entered its data via this process, it may forward the encapsulating file to its outside ad agency. The ad agency uses the file similarly, adding its particular information, and forwarding the file to the server. The server updates the database record accordingly, adds the ad agency to its email distribution list for encapsulating files, and dispatches the latest version of the file to Wired, Nike, and the ad agency.

A pre-press house may be the next party involved, and so forth.

Identification of the URL to which the watermark ID corresponds, and updating of the database record accordingly, may not happen until near the end of the process.

At any time, any of the parties can provide additional information to the database, and share such information with others, via the same process. (Some information may not be suitable for distribution to all involved parties, and can be flagged accordingly.)

Server 19 needn't always be the hub through which all communication takes place. The file as updated by Nike, for example, can be forwarded by Nike directly to its ad agency. The ad agency can add its information, and then provide the twice-updated file to the server, etc.

By using distributed files as proxies for the actual database record, a number of advantages accrue. One is local availability of the latest information by all parties without the need for an internet connection. Thus, if a creative director wants to work on the beach, or otherwise disconnected from the net, the needed information is still available. Another is the ease of integrating software tools at each of the parties with a file of local data specific to a particular advertisement, rather than requiring the architectural hassles of interfacing with a remote database and navigating its attendant authentication and security hurdles.

While the foregoing discussion made reference to emailing files, a typical email program would not normally be used. Instead, to better manage the attendant logistics, a specialized file management/mail program is used by each of the parties. Such program would track the latest file for each advertisement, making same readily available for updating as desired, and index the files by various content fields. The user interface could thus present a list of files, grouped or sorted by any of the database fields, permitting editing or adding of information just by clicking on a given field or tab.

Of course, the file-distribution system just-described isn't essential to the system. A great variety of other arrangements can naturally be employed. One is for each party to log-on to server 19 as needed to inspect, or update, database fields for which it has appropriate permissions.

Numbering Schemes

The payload information encoded into objects (e.g., by watermarking) can take a number of forms and sizes. Four exemplary classes are discussed below:

a) Domain-based payload segmentation;

b) Customer/usage-based payload segmentation;

c) Unsegmented payload; and

d) Unique ID

Domain-Based Payload Segmentation

Domain-based payload segmentation approaches divide the payload into fields, each with a distinct meaning. The CLASS/DNS/UID arrangement earlier detailed is exemplary of this type of approach.

Consider a payload of 60 bits. Twelve bits may form a Class ID. These bits serve as an identifier for a top-level domain. 24 other bits may form a DNS ID. These bits identify an intermediate level domain. Together, the Class and DNS IDs fully identify the class of objects from which the data originates, the

customer, and the server that should respond to the payload. (Some responses may be handled by the client computer, rather than dispatched to a remote server.)

The remaining 24 bits are a User ID, and serve as the most granular identifier, indicating the particular source of the payload. Based on this ID, the responding server knows exactly which response is to be provided.

This payload is embedded, in its entirety, into the customer's object. When sensed by the client computer, the application 28c parses (decodes) the payload into Class ID, DNS ID and User ID fields. The Class ID is used to trigger one or more of the client- or server-side programs. Once "launched" these products then use the Class ID in conjunction with the DNS ID and the User ID to complete the desired action.

One of the Class IDs may signify the object is a magazine page. Based thereon, the application 28c may direct the payload to the router/handler described above for response. Another Class ID may signify that the object is music. Again, the application may direct the payload to the same router. Or the application may direct the payload to a service maintained by a music industry consortium for response. Still another Class ID may signify that the object is a grocery package, and the payload should be routed to an on-line grocer for response. Yet another Class ID may signify that the object is a business card, and the payload should be processed locally, at the client machine. The mapping between Class IDs, and the corresponding response mechanism to which the application 28c should direct the payload, may be maintained by a database associated with the client computer's operating system (e.g., the Windows Registry), as detailed earlier.

Once the payload has been dispatched to a proper response destination, that entity examines the DNS ID to further classify the correct responding entity. For example, different IDs may correspond to different classes of servers within a tree of servers.

One the payload has been directed to the correct class of servers, the User ID defines the terminal "leaf" in the tree (e.g., a database record) that finally defines the response.

Customer/Usage-Based Payload Segmentation

A second approach again employs a segmented payload technique. In this arrangement, however, a first field defines the interpretation of the following bits (e.g., their segmentation into different fields).

Again, consider an exemplary payload of 60 bits. Twelve bits can be a Version ID. These bits indicate how the succeeding bits are to be parsed and interpreted, and may indicate (like the Class ID in the foregoing approach) the particular application program 28c that should be used. The Version ID bits thus serve to indicate the payload type. In the illustrated embodiment, one of these types signifies that the payload is coming from a magazine page and should be handled accordingly. In this case, the remaining 48 bits can be parsed into three fields: Owner ID (15 bits), Publication ID (15 bits), and Media ID (18 bits).

The Owner ID identifies the customer to whom the watermark is registered (e.g., Nike). This is used for ad effectiveness analysis and billing purposes. The Publication ID identifies the particular publication (e.g., July, 2000, San Francisco edition of Wired Magazine). The Media ID identifies a particular page location within that publication.

As before, the payload is embedded in its entirety into the customer's object. The payload is first parsed to determine the Version ID. If the user's device 12 has been programmed to handle such objects locally, further parsing is performed in accordance with data corresponding to that Version ID, and associated processing of the parsed data is performed. If the device has been instructed to dispatch such payloads to remote locations for service, the complete payload can be dispatched with only such further parsing (if any) as may be required to correctly identify the corresponding remote servicing entity.

Unsegmented Payload

An unsegmented payload consists only of two parts: a Version ID (as described above) and an Object ID. In an illustrative case, a 60-bit payload is again used, with 12 bits serving as the Version ID, and the remaining 48 serving as the Object ID.

In this approach the relationships of owner/customer, publication, issue, and media are all maintained in database 17 rather than literally represented in some fashion within the object identifier.

Unique ID

This case is akin to the unsegmented payload, but consists of just a single field – a unique identifier. The same application 28c is always used, and always treats the payload data consistently (e.g., processing locally, or dispatching to a predetermined destination) regardless of the payload contents.

Combinations and hybrids of the foregoing approaches can of course be used. Moreover, the 60 bit payload length is illustrative only. Longer (e.g., up to 1024 bits) or shorter (e.g., down to 8 bits) payloads can naturally be used.

In a particular embodiment, a 32-bit unsegmented payload is used, consisting of 10 bits of payload type and 22 bits of watermark serial number. Some materials (e.g., advertisements including composite graphics) may be encoded with several serial numbers. The mapping between this payload and the customer/publication/etc., is maintained in database 17.

(As noted below, the data sent from the application 28c typically includes information other than the identifier payload, e.g., the type and version number of the application 28c, the electronic address of the dispatching application, etc.)

Router

The router 14 permits any number of different products to be used by the indicia detection and response model. By keeping this function separate and generalized, new products can be added without

design changes to the existing products or the product handlers 16. There are two keys to making this approach successful – speed and flexibility. By using a standardized, open interface, the router is able to facilitate both of these goals.

A premise of an exemplary interface is an enveloping technique that allows the router to "open" the outer transaction envelope and extract the vendor and application ID without decoding the remainder of the transaction (message). Given these two pieces of information, the router uses a simple lookup table to determine the product handler appropriate to complete the transaction. The router then passes the vendor, application, remainder of the transaction and the Internet "reply to" address on to the appropriate product handler. The simplicity of this handling keeps the routing delay to a minimum, while deferring the actual response processing to vendor/product-specific handlers. By including the "reply to" address in the data passed on to the product handlers, the router is freed from the responsibility of return routing for the product's response(s).

To review, the router:

1. decodes the request packet received from the client products into the packet's base components – Vendor ID, Application ID and message;

2. validates the request packet base components against a list of known, good values;

3. if a request packet component is found to be invalid, issues an error message noting the invalid components and returning same to the calling session (e.g., product);

4. sends the decoded request packet contents and any required identification of the calling session to the appropriate product handler; and

5. reports any errors encountered, including invalid packets received, to a system monitor.

Certain data flows associated with the router are shown in Fig. 5.

<u>*Product Handler*</u>

The primary function of the illustrative product handler 16 is to process requests received from the application 28c, via the Internet and router 14, and return the requested information/action to the originating device 12. In the illustrated embodiment, the information requested is the URL associated with the watermark payload sent by the application. In other embodiments, other actions and/or information may be requested.

Each received watermark payload is validated using information in the database 17. If the watermark payload ID is found and is active, the requested action is performed. If the watermark payload ID is not found or is in an inactive state, an error message is returned to the requesting application.

All requests are logged in a transaction log for tracking and billing purposes. This includes any secondary payload information (zip code, Demographic Household ID, etc.) passed in by the application 28c. The log can be maintained by the product handler 16, or elsewhere.

To speed system response, the product handler 16 may anticipatorily send URLs to the application corresponding to watermark payloads the handler foresees may be coming. These URLs can be cached in memory associated with the application 28c, and quickly recalled if needed by the application.

Consider, for example, a magazine containing watermarked advertising. If the user presents a first ad to the device 12, the watermark is decoded and forwarded to the product handler 16, which responds with a URL corresponding to that ad. The application 28c then passes that received URL to a web browser 28b on the device 12, which initiates a link to that internet address. But the handler now knows the magazine the user is reading. By reference to the watermark first received, the handler may discern, for example, that the user is reading the San Francisco edition of the March 14, 2000, Time magazine, and just looked at page 85. Based on this information the handler can query the database 17 for URLs associated with other advertising in that issue. (The database index is structured to permit fast queries identifying all ads in a given magazine issue or other collective data source.) These URLs are passed back to the application 28c and cached. If the user next presents an advertisement from page 110 to device 12, the application 28c finds it already has the corresponding URL locally cached. The application then passes the corresponding URL to the web browser. The web browser initiates the link immediately, obviating a data round trip between the application and the remote system.

The caching can be optimized in a variety of ways. One is to first send URLs corresponding to pages that are next-expected to be encountered. For example, if the user just presented page 85 to the sensor 22, after sending the URL for that page, the handler 16 would next send the URLs associated with pages 86, 87, etc. On sending the URL for the last page of the magazine (typically the rear cover), the handler could start from the beginning (typically the front cover) and send further URLs up to that for page 84. Another optimization is to first cache URLs for the most conspicuous ads, e.g., first send URLs for any 2-page spread ads, then for each full page add, then for each successively smaller fractional-page ad. Still another approach is for handler 16 to dispatch URLs to device 12 for caching in accordance with a contractually-agreed priority. One advertiser, for example, may pay a premium ad rate in exchanged for being cached before other advertisers who don't pay the premium. Other caching priorities, and combinations of such priorities, can naturally be employed.

In some systems, the advertisers or publishers may be charged for use of the system based on the number of URLs served by the system for linking. If local caching of URLs (e.g., at device 12) is employed, it is desirable for device 12 to report to router 14 (or handler 16) the URLs that are actually retrieved from the local cache and used for linking, so that the remote system can log same. Thus, each time the user presents an object to sensor 22 for which a corresponding URL is already cached, application 28c dispatches a message to router 14 reporting the event (and, usually, the particular URL involved). This event is then logged in the transaction log.

This anticipatory dispatching of URLs is one alternative function that may be performed by a product handler. Another is if the application 28c queries the product handler to determine if a more

recent version of the application is available for download. If so, the application – through interaction with the user – can request that the product handler respond with a software download.

In greater detail, application 28c can periodically query the product handler as to the identity of the latest version of application 28c (e.g., the first time the application is used each day). Device 12 may have version 3.04, and the remote system may respond that version 3.07 is the most current. In such case the application 28c can alert the user – by suitable text, graphics, or other means – that a more recent version of the program is available, and query whether such updated version should be obtained. If the user so-instructs, handler 16 can serve to device 12 the latest version of the application (or a patch permitting the presently-installed version to be updated).

Sometimes it may not be necessary to update the application version. Instead, data from the remote system may indicate the desirability, or necessity, or changing just one or more parameters in the application 28c. For example, new security keys can be dispatched periodically by handler 16 to device 12, and used to change the security configuration of the application. Or the application 28c can be instructed to direct further outgoing watermark traffic – either for the next hour, day, or until instructed otherwise - to a different router 14. Such instruction can be used to optimize system performance, e.g., for router load balancing purposes, to avoid internet routes that are found to be slow, etc.

In summary, the detailed handler:

1. validates the received identifier (e.g., watermark serial number) against the list of active identifiers; and, if the serial number is not found, return an error message to the calling session, and log the error to an error handling routine;

2. for each received, valid watermark serial number, finds the corresponding active primary action from the database;

3. for each received, valid watermark serial number, if the handler finds the corresponding primary action is currently not active, it performs an alternative, "default" action instead;

4. if the handler finds an active primary action associated with the received valid watermark serial number, it returns the URL for application use in redirection (round trip approach), or serves the HTML page found to the calling session;

5. if the handler does not find an active primary action associated with the received valid watermark serial number, but does find an associated default action, it returns that URL for application use in redirection (round trip approach), or serves the HTML page found to the calling session;

6. if the handler does not find a valid, active primary or default action associated with the watermark serial number, it returns an error message to the calling session, and logs the error to the error handling routine;

7. records each transaction, including those that result in error messages, for billing and analysis purposes (in other embodiments, this function may be performed by the router, instead);

8. responds to a "software version request" by returning the most recent available application software version number to the calling session;

9. responds to a "software download request" by initiating a file transfer of the most recent available application software to the calling session;

10. responds to a valid Request for Registration packet upload (proper format, an existing serial number, an account ID and a valid corresponding account password) by returning a current registration packet for the provided watermark serial number;

11. responds to an invalid Request for Registration packet by returning an error message to the calling session noting the failure;

12. responds to a local transaction cache flush request by writing the locally cached transactions to the transaction log; and

13. responds to a multiple URL request by returning the URL associated with the provided serial number first, followed by all other active serial numbers and URLs for the publication, issue and region code (optional) provided.

Certain of the above-described processes associated with the product handler are shown in Fig. 6.

URL Performance Monitoring

Returning to operation of the system, the URLs identified in database 17 may, from time to time, become inoperative or impaired due to equipment problems at the remote web site or otherwise. If desired, the handler 16 (or another component of the system) can be programmed to periodically test each of the links registered as active in the database (e.g., once per day), and measure the time for the associated web page to load. If the web page doesn't load, or takes much longer to load than usual (and re-tests confirm that the condition isn't an anomaly), those conditions can be flagged in the corresponding database record. If the handler is requested to provide such a URL to a device 12, the handler can send a message – either with or without the URL – indicating to the device that the URL is misbehaving.

If the URL is working, but is unduly slow to load (either compared to its historical performance, or compared to other URLs), handler 16 can provide an interim diversion to the device 12. For example, it can instruct the device to launch a second browser window, and direct that browser to an alternate destination to entertain the user while waiting for the intended page to load. When the intended page is finally loaded, the first browser window can be displayed - either by closing the second, diversionary window, or by bringing the first window to the front while keeping the second window alive in the background.

This alternate destination is desirably a low bandwidth page, so that it will not unacceptably further slow loading of the desired URL. This alternate page can be one selected by the handler, for which the URL is sent after the desired URL. Or instead of providing a URL from the handler, the handler can serve an HTML or other page directly to the device 12. Or the alternative URL can be stored at device 12

and used to invoke the second browser window upon receipt of data from handler 16 indicating that the desired content will be slow in coming. In some embodiments the user can identify several alternate URLs (e.g., weather, stock info, jokes) and the handler or the application 28c may select among them randomly or otherwise. Or an HTML page or other application can be loaded locally at the device 12 in response to a "get ready to wait" indication from the handler 16.

If a URL is marked in the database 17 as slow or inoperative, the scanning operation periodically rechecks the URL to see if its status in the database should be changed (e.g., changed from inactive to active). Inactive URLs are reported to the registrant by email, and flagged for manual follow-up if not restored to action within a predetermined period.

Illustrative Responses by Product Handler

Part I, above, provided a sampling of the great variety of diverse applications enabled by the illustrated system 10. A few more are detailed below.

Consider use of the system 10 to enable personalized greeting cards. A greeting card company may prepare watermarked press-on stickers for use with its cards or other correspondence. The customer shows the sticker to a camera-equipped computer (either at the retail store, at home, or elsewhere). The computer decodes the watermark and sends same to a corresponding product handler 16 through the router 14. The handler – recognizing the watermark as an unregistered greeting card sticker – invites the customer to enter a destination URL, such as the customer's personal web page. This information is entered by the consumer and forwarded to the remote system for entry in the registration database 17. Thereafter, whenever the sticker is shown to a suitably-enabled system (e.g., by the card recipient), a browser window is automatically launched and directed to the web page specified by the purchasing consumer. (The same result can, of course, be effected without use of stickers, e.g., by encoding the greeting cards themselves.)

In some applications, the product handler may have a library of different responses it can provide to a user in a particular context, depending on the user's further selection. Consider a university student having a suitably-watermarked university ID card. When the card is presented to a device 12, the product handler replies with HTML instructions causing an options menu to appear on the device screen, e.g:

1. *Review calendar of upcoming university academic events*
2. *Review calendar of upcoming university sporting events*
3. *Review present class schedule*
4. *Select courses for next semester*
5. *Review grades*

When the student makes a selection (e.g., with a mouse, or by moving the ID card in a specified manner), the application 28c dispatches data corresponding to the selected option to the product handler, which then responds with the requested data.

In some cases (e.g., Review present class schedule, Select courses for next semester, Review grades), care must be taken to protect such information from persons attempting access using lost or stolen IDs. Accordingly, when any of these options is selected, the handler 16 may first respond to device 12 by querying for a password or PIN. Only after entry of the correct password/PIN is the requested action performed. (For security reasons, the university may prefer that the password authentication process be performed by a dedicated on-campus server, rather than by product handler 16. Naturally, this and other tasks can be delegated to processors other than handler 16 as best fits the situation.)

In other cases, an option menu needn't be presented – the correct response is inferred from the context or environment. Consider a drivers' license that is watermarked with identification of the owner. If presented to an email kiosk 12 at an airport, the decoded watermark may be used to look-up an email account corresponding to that individual, and download new mail. If the same drivers license is presented to a check-in kiosk, the decoded watermark may be used to look up that person's flight reservation and issue a seat assignment. In both cases the kiosks can be essentially identical. One, however, identifies itself to the router/product handler as an email kiosk, the other as a check-in kiosk. The response undertaken by the router/product handler differs accordingly.

Returning to the university example, there may be cases in which students are tempted to swap photos on a student ID, e.g., to permit an imposter to take a graduate school qualifying exam on behalf of a less-qualified student. In the usual case, such photo-swapping may be difficult to detect. This problem can be combated by an exam check-in procedure that includes having each student present their ID to a device 12. An application 28c specialized for this task can forward a watermark decoded from the ID photograph to a handler 16, which responds by causing an image of the identified student to be displayed on device 12. (The university could compile the requisite database of student images as it issues ID cards.) If the exam proctor sees an image on the device that does not match the image on the ID card, appropriate action may be taken. (This arrangement is applicable wherever photo ID documents are used, including airport check-in, customs, immigration, etc.)

Still another application of the illustrated system is to look-up, or act on, meta-data associated with a marked object. Consider an image, video, or audio file that a user downloads from the internet. Familiar applications such as Microsoft's Windows Explorer (including Internet Explorer) may be configured with watermark decoders activated, e.g., from a Properties panel (accessed, e.g., by right-clicking on the file icon or name and selecting the "Properties" option). When a watermark is detected in a file, the Explorer application can send a corresponding packet to a remote system (e.g., the depicted router/product handler/database). The remote system recognizes the packet as originating through the Properties panel of Windows Explorer, and looks-up the watermark ID in a database 17. Meta-data corresponding to the file (e.g., proprietor, creation date, licensing terms, exposure data, subject, etc.) is returned from database 17 (or from another database identified by the router, handler, or database) to the application 28c, and is displayed in the Properties panel (optionally under an appropriate "tab").

(The present assignee has long offered a "MarcCentre" service that serves as a clearinghouse through which watermark identifiers found in photographs, etc., can be used to identify the proprietors and associated information corresponding to such objects.) In embodiments of the present utilizing this service, the router 14 passes the request to MarcCentre server (a product handler in this instance), which provides the solicited information back to the originating application. The present assignee's MarcSpider service complements the service provided by the Media Commerce product. The MarcSpider service constantly scans Internet sites evaluating each graphic encountered to determine whether it contains a watermark. (Audio and video can be similarly analyzed.) With each detected watermark, the MarcSpider service records the graphic file name, size, format, date/time and URL where the graphic was found. This information is then made available to MarcSpider customers in report form.)

Instead of simply displaying the meta-data, the application and/or the remote system can make use of it. For example, if the meta-data indicates that the proprietor of a watermarked image is Corbis, and that the image can be licensed for a certain use under certain terms, the remote system can be utilized as a licensing server – receiving payment information from the user, granting the license, and forwarding transaction details to Corbis.

Still another application is the sale or promotion of music or video over the internet. Taking the case of music, an artist may freely distribute a low-fidelity (or otherwise corrupted or abridged) version of a song. The low fidelity can be by reason of bandwidth limitation (e.g., 500Hz – 2.5 KHz), monophonic (as opposed to stereo), or otherwise. The artist can seek to distribute the low-fidelity version as widely as possible, to serve as a marketing agent for the artist's other works. (The free distribution of lower-bandwidth audio may serve to alleviate some of the network bandwidth problems faced by universities whose students actively engage in transferring free music over the internet.)

Each low-fidelity version can be processed to extract an identifier (e.g., a steganographic in-band watermark; a numeric ID or song/artist name field in a in a file header; a 128-bit hash value obtained by applying a hashing algorithm to the music data, the music file header data, a portion thereof, etc.) If a listener is interested in obtaining a full-fidelity version of the work, the listener can operate a suitably programmed computer or music appliance that extracts the identifier from the work and passes it on to the remote system. The remote system can respond in various ways, e.g., by providing a full-fidelity version of the same work back to the user (such as MP3 download) and charge the user's credit card a fee (e.g., $0.99); or by directing a web browser on the user's computer to an e-commerce/fan web site associated with the music, etc. Such functionality can be provided in general purpose programs such as Microsoft's Internet Explorer, e.g., by right-clicking on a file to obtain a menu that includes this and related functions.

Figs. 8-10 show a sequence of screen shots from such an embodiment. In Fig. 8, a user has right-clicked on an MP3 file icon in a directory listing 200. A property menu 202 pops up that includes, as its second option "MP3Bridge."

Fig. 9 shows what happens when the user selects the MP3Bridge option. An MP3 player 204 is launched, and a dialog box 206 appears. The dialog box queries the user, "More Information About the Artist? Yes No."

Fig. 10 shows what happens if the user selects "Yes." The software sends the identifier – extracted from the MP3 file – to the remote system. The remote system responds with the address of an associated web page, and instructs the user's computer to launch a new browser window directed to that page.

The same functionality can naturally be invoked through the user interface of the MP3 player (or a Windows MediaPlayer, etc., rather than through Internet Explorer). The music application can spawn a separate window, or present the options and the associated data within the existing window.

Yet another application of the remote system is as a "net nanny" filter. Links requested through the system can be checked for keywords, adult-content flags, content ratings, or other indicia of age-suitability, and provided to the requesting computer 10 only if they meet certain earlier selected criteria.

Again, it will be appreciated that the foregoing examples are but a few of myriad applications enabled by the detailed system.

Reporting

System software may enable the provision of customer-accessible reports (accessible over the internet) that show detailed and summary usage information by date, customer, publication, issue date, region, product/version, etc. These reports can be both regularly scheduled and ad-hoc. The specification of the content, relationships and the timing of the reports can be defined by the customer on-line.

Illustrative reports detail:

a) Hit rates/Transactions per customer per ad

b) Hit rates/Transactions per customer per publication per ad

c) Hit rates/Transactions per customer per publication per issue per ad

d) Hit rates/Transactions per customer per publication per issue per region per ad

e) Hit rates/Transactions rates by originating application (28c)

f) Hit rates/Transactions by originating application vendor

g) Hit rates/Transactions rates by originating web domain (e.g., aol.com)

h) Hit rates/Transactions rates by postal/zip codes

i) Hit rates/Transactions by country

Additional marketing/marketplace reporting can also be produced for internal analysis by the service provider, and for sale to other entities. These reports typically provide a more global view of the impact and usage of the system. Using information stored in a demographic database, in conjunction with these usage patterns, the system can provide customers and research agencies with more detailed demographic/statistical data on the system's usage and effectiveness.

In an illustrative system, certain statistics in the demographic database are compiled using statistics from a sample of users that consent to have their activities tracked in some detail, in consideration for certain perks (e.g., give-away cameras, bar-code scanning pens, or other devices, etc.). These users are termed Demographic Households. A software program included in the systems solicits information detailed in the following table from such users over the internet, with a web-enabled interface. A related program allows such users to update/edit their user/household information previously entered. Each such session is password authenticated for security.

User Information	***Comments***
Name	
Address	
Street	
City	
State	
Country	
Postal Code	
Phone number	
E-mail address	
Household Annual Income	*Provided as raw $ or as a selection from a range of numbers*
Occupation	
Education	*May be per member of household.*
Profession	*If applicable*
Number of members of household	
Member of household	
Age	
Sex	
Internet user?	
User of this linking service?	
Internet usage per week	*In hours. Sum of entire household*
Internet business usage per week	
Primary Internet usage?	*Typical household use of the Internet. May be a selection list*
Owned a computer since?	*Year only*
Number of computers in the home?	
Types of computers in the home?	*Mac, PC, etc. Select all that apply*
Rooms where the computers are located	*Home office, bedroom, etc. Select all that apply*
What ISP do you use?	
What is your modem speed?	*Select from list that includes ISDN, ADSL, cable + dial up modems.*
Are you willing to be an official "Demographic Household" and allow us to contact you for feedback on our products and advice on new products?	
What other technology devices do you have in your household?	*Scanners, PC cameras, digital cameras, DVD, PDAs, etc. Select all that apply*

Audio and Video

As with paper advertisements, the illustrated system provides users of web-connected PCs or other appliances with methods of obtaining information, content, associated products, or associated services using the same principles as detailed above.

For example, an application 28 can "capture" music or other audio using a recording device (note recorder, microphone connected to PC, MP3 player, etc.) and analyze the captured audio to detect an embedded watermark. Once detected, the application passes some or all of the watermark payload information, together with identification of the application and its vendor, to the router. The router forwards the payload information to a handler corresponding to the application. The response of the product handler varies with the context and nature of the data. For example, the handler may return the artist, title, track, album, web URL and purchasing information, to the user. Recorded news and entertainment segments may include transcripts (audio, video and/or text) of the segment along with other related web site information. The handler may simply cause the device 12 to launch a browser window directed to a music commerce web site where the music can be purchased.

Security

The system's basic security philosophy is to grant access to each customer's information only to the users authorized by the customer. To this end, the system desirably should:

1. Create and maintain a list of authorized users (accounts).

2. Employ security methods to deny access to any unauthorized users.

3. Limit users to access only the objects they are authorized to access (typically, the objects belonging to that customer).

4. Report and record all unauthorized access attempts.

5. Maintain a log of all authorized user logins (sessions).

6. Provide the capability for the watermark registrant to grant access rights to other accounts (such as ad agencies and pre-press houses).

7. Establish initial passwords for each account

8. Provide the capability for each authenticated user/account to change their password

9. Provide the capability to reset an authenticated user/account's password in the event the current password is lost.

10. Store all passwords as encrypted values (to prevent theft of passwords).

11. Provide the capability to restrict the creation, modification, deletion, and listing/viewing of account information to authorized users.

Audit Trail

Because of the financial implications of the system's activities, all changes to any registration or customer data need to be recorded. This audit trail provides the operator and its customers with an accurate accounting for the current and previous states of the data.

The audit software desirably records the creation, modification, and deletion of all registration and customer data. The audit software also records the username, date/time of creation/modification/deletion of records, and – for modifications – the before and after images of the data changed.

Application-to-Product Handler Interface Definition

The basics of the interface between the application 28c and the handler 16 are (a) a flexible request and response package structure, and (b) a defined connection method based on industry standards. The illustrated messaging employs the http and/or the https protocol to send and receive messages among the system components. An overview is provided in Fig. 4.

Message Format

The message format is XML-compliant and is defined by the following XML DTD –

```
<!DOCTYPE list [
<!ELEMENT Content (vendor, appl, prod)>
<!ELEMENT vendor (#PCDATA)>
<!ELEMENT appl (#PCDATA)>
<!ELEMENT prod (#PCDATA)>
]>
```

The application 28c appends its data to this header for transmission to the product handler 16. Exemplary messages and product handler responses are detailed in the sections that follow.

Application Message Definitions

The application message definitions can be broken down into Request Code, Primary and Secondary information.

*The **Request Code** instructs the product handler 16 to take a specified action.*

*The **Primary information** portion contains the data required to properly service the application's request. The Primary Information varies based on the Request Code.*

*The **Secondary Information** is intended for use by analysis and reporting tools and does not instruct nor aid the product handler in servicing the user's request. Secondary Information contents change based on the Request Code and not all Request Codes are required to have associated Secondary Information. In addition, most of the Secondary Information requires the consumer to grant express consent to its collection. If that consent is not given, the application does not send Secondary Information. A special case exists for selected, consenting consumers to become part of a demographic database.*

Primary and Secondary information may change by request type, but in general conform to the definitions below. The generic format for the product handler is also defined below.

Primary Information *includes the Application Version, Watermark Type, Watermark Serial Number, Context and Environment.*

?? *Application Version: used by the product handler to modify its actions, typically for backwards compatibility*

?? ***Watermark Type: top 9 bits of the illustrative watermark payload. Used by the product handler in processing the Watermark Serial Number***

?? *Watermark Serial Number: remainder of the watermark payload. Provides the index used by the product handler to access the watermark in the registration database*

?? *Context: instructs the product handler to modify/refine its action based on the consumer request's context*

?? *Environment: instructs the product handler to modify/refine its action based on the consumer request's environment. (The environment may be specified, e.g., as home, office, car, portable appliance, etc.)*

Other Request codes can, of course, be used. Each may have its own list of mandatory and optional Primary Information fields. Optional fields are excluded from the primary Information when there is no value associated.

Secondary Information*:*

?? *Demographic Household ID: identifier for a selected demographic group. This is used as an index to the actual demographic*

?? *Input device: Manufacturer, model and version of the device used to detect the watermark (e.g., a TWAIN driver string)*

?? *Operating System: operating system in use on the consumer PC*

?? *Processor: processor type/class on the consumer PC*

?? *Processor speed: processor clock speed, in MHz, of the consumer PC. (May be entered by user, or auto-detected.)*

?? *Language: preferred consumer spoken language*

?? *Country: Country where the consumer PC resides*

?? *Postal Code: Consumer's postal code (used along with the country to pinpoint the location of the consumer).*

(In addition to these explicit data, the packet sent from the device 12 also conveys an IP address (inherent in the use of http protocols) so that the remote device (e.g., the router/handler) has an address to which it can respond.)

Response from Product Handler

```
RtnCode          - Success =1
URL              - the active URL for the watermark serial number
                 received
                       or
RtnCode          - Error <0
Error Message    - text.
```

Request for URL

Required Inputs

Header (XML format)

```
Vendor      (e.g., = Digimarc)
Appl        (e.g., = MB)
```

Data

Required information –

```
Req         =RFU
Ver         = application version number
Type        = watermark type number
Ser         = watermark serial number
Cxt         = context
Env         = environment
```

Optional Information –

```
Ctry        =User's Country name
Lang        =User's preferred Language
HHID        =Demographic Household Identifier
Det         = TWAIN string of the sensing/detecting device
OS          =User PC Operating System string
Proc        =User PC processor type and class
Speed       =User processor speed
Zip         =User postal code
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFU
Type=1
Ser=10001
Ver=1.0
Cxt=A
Env=Q
```

```
Ctry=USA
Lang=English
HHID=1234567
Det=TWAIN string
OS=Win98
Proc=Pentium III
Speed=500
zip=74008-1234
```

Response from Product Handler

```
RtnCode=Success/Error number (Success = 1)
URL=URL associated with specified watermark type and Serial number
Exp=Expiration date/time (GMT) for caching purposes - format of
mm/dd/yyyy hh:mm:ss
```

or

```
RtnCode=Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-1 Type and Serial Number OK, but no URL in database (both the primary and default URL are missing)

-2 Type and Serial Number OK, but URL is marked as inactive (neither the primary nor the default is active)

-3 No record in database matching the Type and Serial Number

-4 Request format error – incomplete data

Request for Configuration

Required Inputs

Header (XML format)

```
Vendor      (e.g., = Digimarc)
Appl        (e.g., = MB)
```

Data

Required information –

```
Req         =RFC
OS          =User PC Operating System
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFC
OS=Win98
```

Response from product handler

```
RtnCode= Success/Error number (Success = 1)
Ver=Latest Application version# available for download
https=yes (or n )
GCURL=URL used to route subsequent Application requests
      or
RtnCode= Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-5 Unknown Operating System

-4 Request format error – incomplete data

Request for Associated URLs

Required Inputs

Header (XML format)

```
Vendor      = Digimarc
Appl        = MB
```

Data

Required information –

```
Req         =RFA
Ver         =application version number
Type        =watermark type number
Ser         =watermark serial number
Cxt         =context
Env         =environment
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFA
Type=1
Ser=10001
Ver=1.0
```

Response from product handler

```
RtnCode= Success/Error number (Success = 1)
Ser1=watermark serial number
Type1=watermark type number
URL1= URL associated with specified watermark type and Serial
number
Exp1=Expiration date/time (GMT)
Ser2=watermark serial number
```

```
Type2=watermark type number
URL2= URL associated with specified watermark type and Serial
number
Exp2=Expiration date/time (GMT)
…..
Ser'n'=watermark serial number
Type'n'=watermark type number
URL'n'= URL associated with specified watermark type and Serial
number
Exp'n'=Expiration date/time (GMT)
      or
RtnCode=Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-8 Type and Serial Number OK, but no associated watermarks or URLs in database

-9 Type and Serial Number OK, but all associated URLs are marked as inactive

-3 No record in database matching the Type and Serial Number

-4 Request format error – incomplete data

Request for Transaction Download

(Needed to account for locally cached redirections. One request per local redirection.)

Required Inputs

Header (XML format)

```
Vendor      = Digimarc
Appl        = MB
```

Data

Required information –

```
Req         =RFT
Ver         =application version number
Type        =watermark type number
Ser         =watermark serial number
Cxt         =context
Env         =environment
```

Optional Information

```
Ctry        =User's Country name
Lang        =User's preferred Language
HHID        =Demographic Household Identifier
Det         =TWAIN string of the sensor device
OS          =User PC Operating System string
Proc        =User PC processor type and class
Speed       =User processor speed
Zip         =User postal code
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFT
Type=1
Ser=10001
Ver=1.0
Cxt=A
Env=Q
Ctry=USA
Lang=English
HHID=1234567
Det=TWAIN string
OS=Win98
Proc=Pentium III
Speed=500
zip=74008-1234
```

Response from product handler

```
RtnCode=Success/Error number (Success = 1)
            Or
RtnCode=Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-4 Request format error – incomplete data

To provide the fastest possible system response, it is desirable that data exchanges between the originating device 12 and the remote system be as short as possible – preferably of a size that can be transported in a single internet data packet (i.e., less than about 536 bits). Such an arrangement avoids the overhead associated with data division on transmission, and data reassembly on reception.

Generally speaking, the combined elapsed time of the system service (i.e., watermark recognition by application 28c, packet delivery to router, decoding by router, handling by product handler, and return of response to application) for a single request should average no more than 3 seconds as measured from receipt of request to 1st byte sent in response to request. Typical speeds are less than 2 seconds, with many responses being provided in less than 1 second.

The immediately following discussion reviews much of the foregoing, but from a different priority case and with additional details.

The MediaBridge digital message is composed of two codes, both of which are embedded in MediaBridge-enhanced images. The media owner code is assigned by the system administrator (e.g., Digimarc) and identifies the entity licensed to add MediaBridge enhancement to images. The routing code

is assigned by the media owner (advertisers, publishers, manufacturers, etc.) and determines where the end-user will be directed when the Client Application reads the MediaBridge codes. Two different advertisements embedded with the same codes can take the end-user to the same web page, while the same advertisement in different publications using different codes can go to different web pages and can be used to track which advertisement or magazine is most effective in bringing end-users to the media owner's web site.

There are three major components of the MediaBridge system. The Client Application is used in homes and businesses by consumers (the MediaBridge end-users) to automatically navigate from an image or object to additional information, usually on the Internet. The MediaBridge Router provides the Client Application with the appropriate Internet address for a given image or object. The Embedding System is used by the media owners to embed the MediaBridge codes into images prior to printing.

IV. MediaBridge Client Application

The Client Application can be distributed via OEM relationships with tethered digital camera manufacturers such as Logitech, 3Com, Creative Labs and others. It is installed by the end-user along with the camera driver and supporting software from the camera manufacturer's installation CD.

The MediaBridge Client Application may run on 200 MHz or faster Pentium or PowerPC computers configured with a tethered video camera under the Windows 95/98/NT 4.0 and Macintosh OS 8.6 operating systems.

The MediaBridge Client Application is initially focused on using MediaBridge-enhanced images to directly browse to additional information on Internet web sites. Therefore, it requires a connection to the Internet, either through a dial-up modem or a permanent connection. However, the Client Application desirably has an extensible architecture that also supports browsing to local data, e.g. on a CD, and linking to other applications.

The MediaBridge system can be used almost anywhere that a video camera can show clear, focused, high-quality images. It operates under lighting conditions varying from dim (about 40 lux) to bright (3900 lux). In very dim light it works with the aid of a supplemental light source, and in bright glare it works if the pictures or objects are shielded from the light source.

1. Operating the End-user Client Application

The first time the Client Application runs it desirably presents the user with a wizard that teaches the best techniques for presenting MediaBridge-enabled images to the Client Application through the video camera. The wizard is tuned for each camera and can use either the sample images or live production images.

Shipped on the installation disk (e.g., CD) can be one or more games that teach users how to best use the Client Application – e.g., focusing the camera, positioning the encoded object in the camera's focal

region, holding the object stationary for the second or so needed for decoding, permissible lighting requirements, etc. The camera box, or inserts inside the box, can be MediaBridge encoded and can link through the browser to a corresponding introductory page hosted by the camera vendor or the system administrator. T-shirts or other prizes may be awarded through the web site, either on a random basis, or upon the showing of proficiency in some aspect of MediaBridge operation.

In an illustrative configuration, the MediaBridge Client Application is always running and is either active or inactive. When active, the MediaBridge video camera window is always on top of any other windows and fully visible, and the Client Application is constantly checking the video for a MediaBridge-enhanced image. When a MediaBridge-enhanced image is found, the appropriate information is displayed - most often as a web page - and the Client Application optionally becomes inactive. When the Client Application is inactive, it hides the video window, releases the camera so it is available for other applications, and uses very little memory or computer resources.

In one implementation, the Client treats the camera as a serially re-usable device. That is, when the Client Application is active and checking the video, no other application can access the video camera. Similarly, the Client Application cannot access the video when another application is using the camera.

The MediaBridge Client Application may include the following functionality:

1) ***Browser/Application Launch**. When a MediaBridge-enhanced image is found, the Client launches the user's web browser or another application. When browsing to an Internet web site, the Client provides the site with the identity of the image and the end-user's zip code, if available. This information allows the media owner's web site to display a localized web page to the user. When launching another application, the Client provides the image owner code and the routing code to the application.*
2) ***Destination menu**. If multiple URLs are specified for a routing code, the Client Application displays a browser-based menu that allows the end-user to chose what page to display, rather than directly navigating to a web page.*
3) ***Branding**. While retrieving the information for displaying a web page, the Client Application displays a local web page that with a pre-stored brand (e.g., Digimarc) and explains that the desired information is being retrieved. This branding page is replaced with the media owner's page without causing any delay to the user. (The contents of the branding page may be updated during Automatic Software Update.)*
4) ***Flexible activation**. When the Client Application is inactive, the user can activate it by:*
   a) *Clicking on the application icon.*
   b) *Pressing a hot-key combination.*
   c) *Clicking on a tray icon. (Windows.)*
   d) *Clicking a button on the browser toolbar.*
   e) *Restoring the minimized MediaBridge Client video camera window. (Windows.)*

5) ***Status display***. *While active, the Client Application provides feedback to the user through the status display pane, which is displayed in the video camera window, next to the view as seen from the camera. The status includes feedback on the ambient lighting conditions, the distance from the camera (if available,) focus, and the current state (preparing to display the image-related information, trying to read the image, or waiting for a MediaBridge-enhanced image to be presented to the camera.)*

6) ***Multiple camera support***. *An illustrative MediaBridge Client Application uses one camera at a time, but can use any MediaBridge-enabled camera installed. If a computer only has one camera, that camera is automatically selected. If more than one camera, the user can select which camera will be used and can change the selection while the Client is running.*

7) ***Automatic Software Update***. *The user can automatically install updates to the Client Application by making a simple menu choice. The Client connects to the Internet, and downloads and installs any available updates. In addition, the Client will suggest checking for updates if it finds a MediaBridge-enhanced image that uses a newer protocol (e.g., by reference to a version indicia encoded with the MediaBridge data).*

8) ***User option configuration***. *Nearly everything in the Client Application can be configured by the user.*

a) Automatically starting the Client whenever the computer starts. (Default.)

b) Activation by hot key.

c) The display of an activation icon on the system tray. (Windows.)

d) Adding a button to the Internet web browser. (Internet Explorer 4 or later, and Netscape 4 or later.)

e) Selection of the last camera used on startup when multiple cameras are installed.

f) Reminder to check for software updates periodically.

g) Running the Wizard at startup. (Default)

h) Automatic deactivation when a MediaBridge-enhanced image is read.

i) Automatic deactivation if nothing is presented to the camera for a specified period.

j) Beep or play sound file upon reading a MediaBridge-enhanced image.

k) Blocking of sites based upon RSACi ratings. Each media owner is expected to self-rate its site using the RSACi scale for the categories of language, nudity, sex and violence. The Router blocks the end-user from a site if the RSACi rating for any category exceeds what the end-user allows. (The Router relies solely on the media owners' self-ratings and does not actually check web pages for RSACi codes.) Selecting this option also results in the display of information about RSACi (http://www.rsac.org/ratingsv01.html) regarding restricting content within the web browser.

l) Automatic connection to the Internet over an existing dial-up (modem) connection.

m) Password protection upon startup.

n) User registration information. (The user is informed that all information is optional and that specific items will be provided to third parties if provided.)

o) The end-user zip code, which the user is not required to provide, is used as a basic piece of demographic information passed along to media owners if it is voluntarily provided by the end-user.

*9) **Wizard**. This wizard provides guidance in setting up a particular camera to obtain the best results with MediaBridge and the best techniques for using MediaBridge as a portal to more information. By default the wizard runs each time the Client Application is started. It also runs the first time a new camera is selected by the user.*

*10) **Camera verification**. When a new camera is selected as the MediaBridge Client input, the Client verifies that the camera is MediaBridge-enabled. If it is not, the user is warned that the camera is not supported and that it may not work correctly with the Client Application.*

*11) **Extensible architecture**. The MediaBridge Client handles reading MediaBridge-enhanced images and connecting to the desired information, usually by displaying Internet or local web pages in a browser window. Its functionality can be extended by MediaBridge-enabled applications that register for the handling of specific data. For example, if a MediaBridge-enhanced business card were presented, the MediaBridge Client could run a MediaBridge-enabled application that downloads business card information from a web site and updates the user's contact list with the new information. Another example would be a page from a MediaBridge-enhanced children's book that causes an audio file to be played for the page.*

*12) **Embedding support**. If the Client Application is being used by a media owner to verify that an image has had the correct MediaBridge codes embedded in it, the Client displays the name of the media owner, the routing information and the relative strength of the MediaBridge watermark when a MediaBridge image is read. In order to protect the privacy of each media owner, this information is only provided if the user is able to provide a valid embedding user name and password for the media owner.*

V. MediaBridge Router

The Router is essentially transparent to the end-user. When the Client Application detects a MediaBridge-enhanced image linked to information on the Internet, it communicates with the Router to obtain the Internet addressing information of the web page to be displayed.

The Router also includes the following functionality:

*1) **Routing information maintenance**. Contained within the Router is information linking each unique MediaBridge code to one or more related Internet addresses. In one implementation, the system administrator (e.g., Digimarc) maintains the routing information using information supplied by its advertising customers. In another implementation, the media owners update the information themselves using a secure Internet connection with the Router.*

2) ***Problem handling***. *If a routing request cannot be satisfied, the Router responds in a way that minimizes the impact on the end-user. For example if the MediaBridge code is unknown, then the Client Application is given the URL for the media owner's home page. In addition, each day the error occurs the Router notifies the media owner by email that the error occurred.*

3) ***Content rating***. *If the media owner has provided RSACi rating information for the image or its site, and the end-user has specified RSACi ratings that specify that the site is to be blocked, the Router returns a web page to the user indicating that the site contains inappropriate content and does not connect to the media owner site.*

4) ***Validation***. *Periodically (e.g., on a daily basis) the Router validates all of the active information in its database. If any errors are found, the media owners are notified by email. If the errors are not fixed with one day, Digimarc is notified. The conditions checked are:*

   a) *Missing URLs on active links.*

   b) *URLs referring to non-existing pages.*

   c) *Pages that exceed the acceptable download time as required by Digimarc.*

5) ***Tracking***. *The Router may log Client Application requests in order to develop marketing information. Such a tracking log could include:*

   a) *Date and time of the request.*

   b) *Media owner and image.*

   c) *Zip code of the end-user, if provided.*

   d) *IP address that issued the request.*

6) ***Reporting***. *Using the tracking information, the Router provides the following reports for use by Digimarc:*

   a) *Number of URL requests for a particular date range.*

   b) *Number of URL requests by media owner for a particular date range.*

   c) *Number of URL requests by MediaBridge-enhanced image for a particular date range.*

(The tracking and reporting are desirably structured to allow media owners to obtain traffic and marketing reports online from the Router.)

VI. ***MediaBridge Embedding System***

The Embedding System includes:

?? *a Photoshop-compatible Embedder Plug-in for embedding the MediaBridge codes,*

?? *a Photoshop-compatible Reader Plug-in for verifying MediaBridge-enhanced digital images,*

?? *the Client Application for verifying MediaBridge-enhanced proof and press prints, and*

?? *an Internet-based Router Maintenance Application for obtaining MediaBridge codes and assigning URLs to MediaBridge codes.*

The Plug-ins require a connection to the Internet only for authorization and to assign new MediaBridge routing codes. The Router Maintenance Application always requires an Internet connection.

1. Router Maintenance Application

The Router Maintenance Application's primary purpose is to assign routing information to the MediaBridge codes so that an end-user is presented with the appropriate web page when the Client Application reads an image.

The Router Maintenance Application includes the following functionality:

1) ***Multiple locations**. A single media owner account can be accessed by different people in different locations. It can also be accessed by people in different organizations such as by an advertiser and its advertising agency.*
2) ***Restricted Access**. Each media owner has the ability to restrict who can access the Router information and can specify who can create new MediaBridge codes, use existing MediaBridge codes, or change the information for routing codes. The media owner can add, change or revoke access at any time.*
3) ***Secure access**. All Internet access to the Router is through secure connections.*
4) ***Routing Codes**. The assignment of new routing codes, changing existing routing and deleting or reusing old routing codes.*
5) ***Time-based routing**. Each routing code can be assigned multiple URLs, each of which can optionally have an effective date and an expiration date that determines when it is to be used in routing. Expired URLs may automatically be deleted by the router after thirty days.*
6) ***Multiple routing**. If multiple URLs are specified for a routing code, the Router returns to the end-user a browser-based menu that allows the end-user to chose what page to display, rather than directly navigating to a web page. In one embodiment, a single routing code may have up to four unexpired URLs. Each URL can have a short description that will be a browser link to the URL, a long description of up to 500 characters, and a URL to an icon to be displayed in the menu. The icon can be no larger than 50 pixels high by 300 pixels wide.*
7) ***Logging**. All changes to the routing information are logged and may be reviewed by the media owner.*

2. Plug-in Overview

The first time embedding is done on a computer for a media owner, the Embedder requires the account number for the media owner, and a valid user name and password as defined by the media owner. The Embedder connects via the Internet to the Router, verifies that the user is authorized, and downloads information about the media owner. Further embedding for that media owner can be performed without connecting to the Router. However, each time the user connects to the Router to obtain routing information for embedding, the Router validates the user name and password against the currently valid

names and passwords. If the previously used name and password are no longer valid, the user has to provide a valid name and password in order to continue embedding for the media owner.

The media owner account number is only needed for the initial authorization since any future verification is done using the name of the media owner as maintained by the Embedder. Since a graphics artist at an advertising agency can work on projects for two or more media owners, a single graphics artist may have different user names and passwords for each media owner.

The Reader Plug-in is used primarily for verification of images after embedding. It restricts access in the same way as the Embedder Plug-in with the additional restriction that it will provide information about an image only if the user can provide a valid user name and password for the media owner. If the media owner information is not available on the current computer, the Reader will connect to the Router for verification.

The plug-ins share this functionality:

1) ***Multiple media owners**. A user can perform embedding or reading for multiple media owners. The user must have a valid user name and password for each media owner.*
2) ***Multiple users**. A single computer can be used by several people. Unless they are using the same user name and password, they do not share information.*
3) ***Automatic Software Update**. The user can automatically install updates to the plug-ins by making a simple menu choice. The plug-ins connect to the Internet, and download and install any available updates.*
4) ***Secure access**. All Internet access is through secure connections.*

3. Embedder Plug-in

The Embedder Plug-in also includes the following functionality:

1. ***Routing codes assignment**. The user selects a routing code to embed from a list of existing codes provided by the Router via an Internet connection. Each routing code is identified by a unique routing number and description. Once selected through the Router the information about a routing code is retained on the local computer until removed by the user.*
2. ***New routing codes**. If authorized, the user can connect to the Router through the Embedder to create a new routing code. The routing code can be created with or without the URL information, which can be added later.*
3. ***Routing code updates**. Whenever the Embedder connects to the Router, it downloads any updates that were made to routing codes being cached locally.*
4. ***Masked embedding**. The user can mask off a part of the image so that the MediaBridge codes are only embedded in the masked area. In one embodiment, different codes are applied in different mask areas. Typically, the user cannot embed different MediaBridge codes in the same part of an image.*

5. ***Variable intensity***. *The user can globally vary the intensity (and thus visibility) of the MediaBridge watermark from light to very heavy, and can also locally vary the intensity in different areas of an image (i.e., the intensity is adapted to local image characteristics).*

6. ***Logging.*** *Each time the user embeds in an image, the Embedder records a log of the date, time, information embedded, the embedding settings (e.g., intensity), the user name, the computer name, and the name of the input image file. The log is a text file on each user's computer. It can be viewed in any text editor.*

4. Reader Plug-in

The Reader Plug-in also includes the following functionality:

1) ***Reading***. *Reads a digital image, which may have been scanned, and, if the user is authorized, displays the media owner, routing information and a measure of the strength of the MediaBridge watermark.*

2) ***Masked reading***. *The user can mask off part of the image and read the MediaBridge information only from that part.*

PART III

Inventive Combinations

<omitted in this Appendix>

5. Conclusion

Having described and illustrated the principles of our technology with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while certain of the embodiments were illustrated with reference to internet-based systems, the same techniques are similarly applicable to any other computer-based system. These include non-internet based services such as America Online and Compuserve, dial-up bulletin board systems, etc. Likewise, for internet-based embodiments, the use of web browsers and web pages is not essential; other digital navigation devices and other on-line data repositories can be similarly accessed.

Similarly, while the details of illustrative systems were particularly given, the underlying principles can be employed in numerous other forms.

For example, one other form is to steganographically encode physical objects with Digital Object Identifiers (DOIs). The Center for National Research Initiatives and the Digital Object Identifier Foundation (www.doi.org) have performed extensive work in establishing an infrastructure by which digital objects can be distributed, tracked, and managed. Some of this same infrastructure and technology can be adapted, in accordance with the teachings provided above, to associate new functionality with physical objects.

Another form is not to reference a remote data repository by data embedded on an object, but instead to encode the ultimate data directly on the object. A photograph, for example, can be literally encoded with a telephone number. On presenting the photograph to an optical sensor on the telephone, the telephone can analyze the optical information to extract the telephone number, and dial the number, without the need for any external data. Similarly, a printed office document (e.g., spreadsheet) can be encoded with the path and file name of the corresponding electronic file, obviating the need for indirect linking (e.g., to a remote database to correlate a UID to a computer address). A person's business card can directly encode that person's email or web address. Most of the above-described embodiments are suitable for such direct encoding of the related data.

In the business card example given above, the detailed techniques can be supplementary to existing optical character recognition techniques. That is, the image data from an optical sensor can be applied both to a Bedoop decoder and to an OCR system. Text characters discerned by the OCR system can be entered directly into a contacts manager personal database. The techniques employed in the Bedoop system to locate the encoded object and handle visual distortion (e.g., the visual artifacts due to scale, rotation, etc.) can advantageously be used in OCR detection as well, permitting extraction of the OCR information without careful placement of the card.

While certain of the foregoing embodiments made reference to ink-jet printing, similar advantages can often be obtained with other printing technologies, e.g., laser/xerographic printing, offset printing, etc.

In the foregoing embodiments, Bedoop decoding generally proceeded from image data obtained from a physical object. However, in some contexts, it is advantageous to Bedoop-decode image data provided electronically, e.g., over the internet.

Likewise, while the foregoing embodiments generally relied on Bedoop image sensors that stared out for an object at an expected point, in alternative embodiments, sensors that seek rather than stare can be employed (as was illustrated above in connection with the elevator example).

Similarly, while the illustrated embodiments generally employed sensors that repeatedly grabbed frames of image data, this need not be the case. Single frame systems, such as flatbed scanners, and video systems arranged to grab single frames -- with or without TWAIN interfaces -- can alternatively be used.

As indicated above, while steganographic encoding of the digital data is used in the preferred embodiments, visible forms of digital encoding – such as bar codes – can naturally be employed where aesthetic considerations permit.

In certain of the embodiments, digital data conveyed by means other than optical can be used. Electromagnetic detection (e.g., of the sort used in proximity-based card-access systems) can be arranged to decode digital data, permitting "at-a-distance" reading of data from physical objects, just as in the foregoing embodiments.

Since the Bedoop image sensors typically acquire plural frames of data, the extraction of the digital data can be based on more than a single image frame. More confidence in the results may be

accumulating decoded data over several frames. Moreover, movement of the object within the sensor's field of view may permit the system to acquire information from other perspectives, etc., enhancing system operation.

While the preferred embodiments employ 2-D image sensors (e.g., CCDs), other optical sensing technology can alternatively be employed. Supermarket laser scanners, for example, can read bar-code data. Raster-scanning of such systems can permit acquisition of 2-D data (either in bit-mapped form, or grey-scale).

Some embodiments can advantageously employ texture-based Bedoop encoding of objects. Bedoop texturing can be effected by various means, including pressure rollers, chemical or laser etching, etc.

It should be noted that the responses triggered by a watermark can be changed over time. This extends the useful life of an encoded object. For example, an encoded link in a magazine ad for a 1999 Ford Explorer that points to a Ford URL related to the 1999 Ford Explorer can be updated to point to the URL for the 2000 model year version when marketing of the new model year vehicles commences.

In other embodiments, of course, a literal URL can be encoded, and can be used to direct a browser or other information appliance to that address. Still further, a literal URL can be encoded, but not necessarily used. Instead, the encoded URL can be mapped to an actual URL (i.e., a URL to which the browser is directed or to which a response to the MediaBridge object is otherwise keyed) through a database. In one such embodiment, a URL is encoded in an object together with a future date. On "reading" the object, the local (client) computer checks the associated date. If the date has not passed, the literal URL is used as the actual URL. If the date has passed, the client computer refers to the code to a remote database (e.g., at the router) to obtain an actual URL (which may be the same – if no update has been required, or may be new). The actual URL is then used in providing a response to the MediaBridge object.

The implementation of the watermark encoding and decoding systems is straightforward to artisans in the field, and thus not unduly belabored here. Conventionally, such technology is implemented by suitable software, stored in long term memory (e.g., disk, ROM, etc.), and transferred to temporary memory (e.g., RAM) for execution on an associated CPU. In other implementations, the functionality can be achieved by dedicated hardware, or by a combination of hardware and software. Reprogrammable logic, including FPGAs, can advantageously be employed in certain implementations.

While the foregoing embodiments have generally employed planar objects to convey the digital encoding, this need not be the case. Objects of other shapes can likewise be employed. Some shapes present relatively straightforward image processing tasks. As noted above, data imaged from a soft drink can or other cylindrical surface can be remapped using known geometrical transforms so as to essentially "unwrap" the printing from the can. Other geometries can present more complex re-mappings, but are likewise generally within the capabilities of the artisan. (Such remapping is facilitated by encoding in the

data certain reference markings, such as subliminal graticules, etc. The unknown 3D shape of the object being imaged can usually be inferred from the apparent warping of the reference markings in the 2D image data generated by the scanner. Once the warping is characterized, it is generally straightforward to un-warp so as to prepare the image data for decoding.)

It was once popular to predict that paper documents would be replaced with electronic media. In hindsight, electronic media may be recognized as a poor surrogate for paper. Electronic media conveys information flawlessly, but is lacking in experiential attributes. We can hold paper, stack it, own it, deface it, give it, guard it, etc. It provides an opportunity for physical dominion entirely lacking with electronic media.

From the foregoing discussion it can be seen that, rather than replacing paper with electronic media, perhaps the future lies in giving paper digital attributes – hybridizing the physical experience of paper with the technical advantages of digital media. Such an arrangement makes available a great wealth of new functionality, now accessible through familiar paper items, rather than through a "computer input peripheral."

In view of the many embodiments to which the above-detailed principles may be applied, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as fall within the scope and spirit of the following claims, and equivalents thereto.

WE CLAIM

1. A method of data processing on a computer system, comprising:

using an application program to compose an electronic version of a text-based document;

printing the document onto paper, the printing including steganographically encoding the printed paper with plural-bit auxiliary data;

storing the plural-bit auxiliary data in association with data identifying a location at which the electronic version of the document is stored.

2. A method of data processing on a computer system, comprising:

presenting a text-based printed document to an optical capture device;

processing image data produced by said device to decode plural-bit data steganographically encoded therein;

based on said decoded plural-bit data, launching a software application corresponding to said printed document; and

using said software application to open an electronic version of said document.

3. In a method of operating a computer, the computer including an operating system with a registry database, the registry database associating specific data types with specific software programs particularly corresponding thereto, an improvement comprising:

providing a frame of image data;

decoding plural-bit identifier data from the image data;

consulting the registry database to identify a software program corresponding to said identifier data; and

invoking the identified software program.

4. The method of claim 3 which includes:

steganographically decoding plural fields of data from the image data, one of said fields comprising the identifier data; and

providing another of said fields of data to the identified software program for use thereby.

5. A greeting card comprising a substrate with visually-perceptible indicia printed thereon, wherein the card is steganographically encoded with plural-bit binary data that can be decoded by an image processing device and used to direct a computer to a web site where an image, video, and/or audio presentation corresponding to said card is provided.

6. A method of providing a customized greeting, comprising:

acquiring a greeting card having plural-bit data steganographically encoded therein;

customizing a web site presentation corresponding to said card;

providing the card to a recipient;

decoding the steganographically encoded plural-bit data from the card; and

in response to said steganographically decoded plural-bit data, presenting to the recipient the web site presentation.

7. A method of printing a magazine, comprising:

processing an electronic representation of an advertisement with a digital watermark to steganographically encode plural bit data therein;

printing a page of advertising in accordance with said electronic representation to yield a steganographically encoded advertisement page; and

binding said page into a magazine;

wherein said plural bit data serves to identify an entry in a database, said database entry having stored therein an internet address of a web page that is associated with said advertisement.

8. A promotional method comprising:

steganographically encoding a print advertisement to hide plural-bit data therein;

processing the print advertisement to extract the plural-bit data therefrom; and

using at least a part of the extracted plural-bit data to direct an internet web browser to a web site that provides consumer information related to a product or service promoted by the print advertisement.

9. A method of determining consumer response to print advertising, comprising:

encoding a first print advertisement with first data;

encoding a second print advertisement with second data different than the first;

the first and second data providing identifiers by which consumer devices can link to web pages associated with said advertisements;

monitoring linking traffic due to each of said identifiers to thereby determine consumer response to the advertisements.

10. The method of claim 9 in which the encoding takes the form of visible bar codes.

11. The method of claim 9 in which the encoding takes the form of steganographic digital watermarks.

12. The method of claim 9 in which the first and second advertisements are identical, except for the data encoded therein.

13. The method of claim 12 in which the first and second advertisements are published in different magazines.

14. The method of claim 9 in which the first and second advertisements are different, apart from the data encoded therein.

15. The method of claim 14 in which the first and second advertisements are published in the same magazine.

16. A promotional method comprising:

presenting an object within the field of view of an optical sensor device, the object being selected from the list consisting of a retail product, packaging for a retail product, or printed advertising;

acquiring optical data corresponding to the object;

decoding plural-bit digital data from the optical data;

submitting at least some of said decoded data to a remote computer; and

determining at the remote computer whether a prize should be awarded in response to submission of said decoded data.

17. A method of interacting with a magazine using a computer, the computer including an internet web browser, the method including:

providing a peripheral device having a sensor;

positioning the peripheral device adjacent a first advertisement in the magazine to direct the web browser to a first internet address; and

positioning the peripheral device adjacent a second advertisement in the magazine to direct the web browser to a second internet address.

18. The method of claim 17 in which the positioning comprises scanning barcode indicia published in said advertisements.

19. The method of claim 17 in which the peripheral device is a camera device having a sensor with rows and columns of sensor elements.

20. A computer peripheral and method of its use, the peripheral being used in conjunction with a computer system having an internet browser associated therewith, the peripheral comprising:

a housing adapted to fit within a user's palm and slide over a medium;

an optical sensor having at least one sensing element and producing optical data;

a lens for imaging the medium onto the sensor;

the method comprising:

sliding the peripheral over a portion of a printed advertisement;

processing the optical data to decode plural bit information encoded on the advertisement; and

using said plural bit information to direct the internet browser to an internet web page associated with said advertisement.

21. The arrangement of claim 20 in which the plural bit information does not comprise a web address, but rather comprises an advertisement identifier, and in which the method further includes:

transmitting said advertisement identifier to a remote computer;

receiving from said remote computer a web address associated with said identifier; and

directing the internet browser on said computer system in accordance with said web address.

22. The arrangement of claim 20 which includes sliding the peripheral over a portion of the printed advertisement having a barcode printed thereon.

23. An electronic commerce method comprising:

providing a printed catalog that includes an image of an article offered for sale by a merchant, wherein the image is encoded with plural-bit binary data;

optically sensing the image to produce optical data corresponding thereto;

decoding the encoded data from the optical data; and

electronically ordering the article from the merchant by use of said decoded data, wherein said ordering makes use of earlier-stored customer profile information.

24. The method of claim 23 in which the customer profile information includes clothing size data.

25. In a wireless telephony handset including a microphone, a modulator, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation, an improvement comprising an optical sensor producing optical data, a lens for imaging an object onto the sensor, and a decoder for decoding plural bit identifier data conveyed by a barcode or a digital watermark on the object.

26. An image-based network navigation method permitting a user to link to a remote computer, comprising:

detecting encoded data from a printed object;

linking to the remote computer through a network in accordance with said encoded data; and

providing the user's zip code to the remote computer.

27. A method comprising:

sensing an object identifier from a first object;

sending said first object identifier from a first device to a second device;

in response, at said second device, identifying address information corresponding to said first object identifier and sending same to the first device;

initiating a link from the first device in accordance with said address information;

at said second device, identifying additional objects related to said first object; identifying additional address information corresponding to said additional objects; and sending said additional address information to the first device;

storing said additional address information in a memory at the first device;

wherein, if an object included among said identified additional objects is sensed by the first device, the corresponding address information can be retrieved from said memory in the first device without the intervening delays of communicating with the second device.

28. An apparatus including a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) an identifier of said software program, and (b) at least a portion of detected machine readable data.

29. The apparatus of claim 28, wherein said packet of data also includes address information identifying the apparatus.

30. The apparatus of claim 28 comprising a detector of digital watermark data.

31. The apparatus of claim 28 comprising a detector of barcode data.

32. An apparatus including a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) a context or environment identifier, and (b) at least a portion of detected machine readable data.

33. The apparatus of claim 32, wherein said packet of data also includes address information identifying the apparatus.

34. The apparatus of claim 32 comprising a detector of digital watermark data.

35. The apparatus of claim 32 comprising a detector of barcode data.

36. A networked computer system, responsive to watermark data sent from a software program on a remote computer, to initiate delivery of advertisement data to said remote computer.

37. A system as described and detailed above.

METHODS AND SYSTEMS FOR CONTROLLING COMPUTERS OR LINKING TO INTERNET RESOURCES FROM PHYSICAL AND ELECTRONIC OBJECTS

Abstract of the Disclosure

Physical or electronic objects are encoded with identifiers, which serve to trigger object-appropriate responses from computer systems that encounter such objects. The encoding may be steganographic (e.g., by digital watermarks), so the presence of such identifiers is not evident to persons encountering the objects. An exemplary application is a computer system that looks at a printed magazine advertisement and initiates a link to a corresponding internet page. In one such implementation, the computer system senses an identifier encoded in the advertisement, forwards the identifier to a remote database, receives from the database a corresponding internet address, and directs a browser to that address. The same arrangement can be used for on-line ordering from printed merchandise catalogs. Another application is a computer system that looks at a printed spreadsheet, and retrieves from disk storage an electronic version of the same document for editing. In one such implementation, the computer system senses an identifier encoded in the printed spreadsheet, checks the identifier against a local index of documents stored on the computer, and recalls the corresponding document for editing. A variety of other applications, and associated methods and apparatuses, are also disclosed.

APPENDIX H

Print Media with Embedded Messages for Controlling Printing

Related Application Data

The subject matter of the present application is related to that disclosed in US Patent 5,862,260, and in co-pending application 09/503,881, filed February 14, 2000; which are hereby incorporated by reference.

Technical Field

The invention relates to printer systems, and specifically, relates to adapting printer performance for different types of print media.

Background and Summary

A challenge facing printer manufacturers is developing cost effective ways to optimize printer operation for a variety of different types of paper. The myriad of paper types available today can exhibit widely varying performance in a printer. For example, in the field of ink jet printing, the absorption properties of different types of paper can significantly impact print quality. If the printer could ascertain characteristics of the paper, it could adapt its operation to the absorption properties of the paper and provide a higher quality printing across a variety of paper types.

One way to optimize printer performance for a variety of paper types is to make the printer operating parameters adaptable to a range of paper types. This leads to another challenge of properly setting the operating parameters for a particular print job. One way to set the parameters is to provide a user interface that enables the user to input paper type or paper characteristics. This, of course, is quite demanding on the user.

Another alternative is to automate parameter adjustment by incorporating technology into a printer to enable it to determine paper type automatically and adapt its operation accordingly. For example, developers of ink jet printing technology have attempted to design sensors to determine paper type so that printer operation can be optimized for the paper. Ideally, the printer should be able to detect paper characteristics such as its thickness, reflectivity, dimensions, absorption coefficient, and bleeding coefficient. While such sensor technology holds promise in improving print quality, building such sophisticated sensor technology is complex and costly.

The invention provides technology for determining print media attributes and adjusting printer parameters using control data embedded in the print media. In particular, a message embedded in the printer paper conveys printer control information to the printer about paper characteristics. A printer, or other system with printing capability (e.g., fax machine, scanner, copier, etc.) uses a sensor to capture a representation of the message signal and automatically decodes printer control information from the

message signal. A control unit in the printer interprets this information and uses it to adjust operation of the printer.

There are several aspects to the invention. One aspect of the invention is a paper medium carrying a steganographic message used to adapt printer operation to the paper medium. The steganographic message includes printer control information related to the paper medium that is readable by a machine. This information is used to control a printer so as to optimize print quality for the paper medium.

Another aspect of the invention is a printer system that adapts the operation of a printer to print media based on control information embedded in the print media. The system comprising an image sensor for capturing an image of print media, a steganographic decoder for reading a steganoraphic message from the image of the print media, and a printer control unit in communication with the decoder. The printer control unit receives the printer control information and uses the information to optimize printer operation for the print media.

Another aspect of the invention is a method for adapting operation of a printer to a type of print media. The method captures an image of at least a portion of a print media, steganographically decodes a message from the image, including printer control information, and uses the printer control information to adapt operation of the printer to the type of print media.

Further features will become apparent with reference to the following detailed description and accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a block diagram illustrating a printer architecture that reads digital watermarks to obtain printer control information.

Detailed Description

The following sections describe methods and systems for using digital watermarks on print media to convey printer control information to a printer. This printer control information may be expressed in many forms. It encompasses paper characteristics and printer control parameters. One form of printer control information is an identifier or set of identifiers that index control information. The printer uses the identifiers to look up corresponding printer operating parameters.

Another form of control information is a set of paper characteristics, such as paper thickness, reflectivity, dimensions, absorption coefficients, bleeding coefficients, etc. Still another form of control information is one or more printer control parameters that control printer operating settings. In an ink jet printer, these settings may include the volume of ink drops, the number of ink drops emitted per unit area, etc. It may also include rendering of the image at the optimum resolution (e.g., dpi) determined by the control information embedded in the paper.

Fig. 1 is a block diagram illustrating a printer architecture that reads digital watermarks to obtain printer control information. The watermarked print media 100 shown in Fig. 1 represents a sheet of paper or other object submitted to the printer. The print media includes a digital watermark that conveys printer control information. A variety of digital watermarking schemes may be used to embed the watermark onto the print media. Some example watermark encoding and decoding schemes are provided in US Patent 5,862,260, and in co-pending application 09/503,881, filed February 14, 2000.

In digital watermarking of physical objects, there is a tradeoff between visual perceptibility and survivability of the watermark. In this application, the watermark is embedded so as to be sufficiently robust to survive analog to digital conversion. The watermark may be encoded by altering the luminance or one or more other color channels of an image on the surface of the paper. Alternatively, the watermark may be encoded using clear inks that modulate the microtopology of the paper's surface or that are readable when exposed to light in non-visible wavelengths, like UV or infrared. Also, the microtopology of the paper surface may be altered in the process of creating the paper so as to embed a watermark. Alternative machine readable codes may be used as well, such as data glyphs, bar codes, etc.

The watermark signal is preferably repeated on the surface of the print media so that a watermark decoder can extract the printer control information from a small and relatively arbitrary portion of the print media. For example, the watermark signal may be repeated across one side or both sides of a piece of paper. If the watermark is slightly visible like a conventional watermark, it may be preferable to place it only on one side of the paper so as not to interfere with content printed on the other side.

In the system depicted in Fig. 1, the printer architecture has an image sensor102 to capture an image of the watermarked print media. As discussed below, the image sensor may be an integrated component of a product with a printer subsystem or a separate component of a computer system attached to a printer. The image sensor transfers the image to a memory device. Depending on the implementation, this transfer may encompass one or more intermediate stages where portions of the image are temporarily buffered, transformed (e.g., color conversion), compressed, uncompressed.

A watermark decoder 104 reads watermarked image data from the memory device, detects the watermark in the watermarked image and extracts a message from the watermark, including any printer control information. The decoder communicates the printer control information to a printer control unit 106, which in turn, interprets the control information and determines the corresponding operating parameters 108 to apply to a print job for the print media.

The printer control unit 106 enforces these operating parameters by issuing corresponding control signals to a print mechanism 110.

The image sensor, watermark decoder and printer control may be implemented in a variety of combinations of hardware, firmware and software.

The image sensor may be implemented using conventional imaging devices such as CCD or CMOS arrays used in scanners and cameras. The sensor may be built into the printer, or may be a

peripheral device, such as a PC camera. In the former case, the image sensor within the printer communicates image data to the watermark decoder. Many printers are subsystems of multifunction devices that have printing and scanning functions. For example, copiers and fax machines have printers, image sensors, and memory for storing an images or portions of an image. In these types of devices, the watermark decoder operates on portions of the image as it is scanned into the device's image memory.

In the latter case, the image sensor may communicate the watermarked image directly to an image memory and watermark decoder within the printer. Alternatively, the image sensor may communicate the image to image memory in a computer, which in turn, either executes a software watermark decoder on the image, or transfers the image to a watermark decoder in the printer. For example, a printer driver executing on a PC attached to the printer may include a watermark decoder to extract printer control information. In this configuration, a user would present the paper to a camera, such as a PC camera, attached to the computer. The printer driver then would access image data in the computer's memory captured from the camera and execute watermark detecting and reading on that image data. The printer driver then either communicates extracted printer control information to the printer, or interprets it on the PC and issues control signals to the printer.

As demonstrated in the examples provided above, the watermark decoder may be implemented within a printer or in a separate device that communicates the printer control information or control signals to the printer. For example, the watermark decoder may be an application program (e.g., the printer driver program) in a computer attached to a printer, or a program implemented in software or firmware in the printer. Alternatively, the watermark decoder may be implemented in hardware within the printer or some other device connected to it, such as a camera, Personal Computer, personal digital assistant, etc.

The printer control unit may be implemented within the printer, a device connected to the printer, or in a combination of both. For example, the control unit may be a programmed processor, such as a DSP, in the printer, a printer driver in a computer attached to the printer, or in a combination of both.

To illustrate the operation of the system, consider an example of a multifunction device that includes an ink jet printer and scanner. The user places blank watermarked paper in the printer and sends a print job to the printer from an attached computer. As the printer loads a sheet of paper to start the print job, it scans an image of at least a portion of it (e.g., the top edge). When sufficient image data fills a buffer in the scanning subsystem, it sends a signal to the watermark decoder, executing within a processing unit on the device. The amount of image data needed to trigger watermark decoding depends in part on the embedding process, and specifically, on the minimum image size required to hold a complete watermark message. For example, if the watermark is repeated in lines or blocks of the paper surface, the image sensor needs to capture an image of at least one line or block.

Operating on the image data, the watermark decoder detects the watermark, reads the message from it, and transfers the printer control information in the message to the printer control unit.. The

printer control unit uses the printer control information as an index in a table to look up corresponding operating parameters. These operating parameters are associated with control signals. The printer control unit issues these control signals to the print mechanism. The print mechanism includes a print head and cartridge that allows for the control of ink drops per a given dot location on the page. Based on the absorption properties of the paper, as conveyed in the watermark, the printer control unit sends a control signal to the printer cartridge that specifies the number of drops to be emitted per dot.

These functions of the printer control unit may be implemented within the same or separate processing unit as the one that executes the watermark decoder.

Concluding Remarks

Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. To provide a comprehensive disclosure without unduly lengthening the specification, applicants incorporate by reference the patents and patent applications referenced above.

The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

I claim:

1. A paper medium carrying a steganographic message, the steganographic message including printer control information related to the paper medium that is readable by a machine from an image captured of at least a portion of the paper medium, and that is operable to control a printer so as to optimize print quality for the paper medium.

2. The paper medium of claim 1 wherein the printer control information includes one or more identifiers that are used to look up printer control information used to optimize printer operation for the paper medium.

3. The paper medium of claim 1 wherein the printer control information includes paper characteristics information of the paper medium.

4. The paper medium of claim 1 wherein the steganographic message is encoded in a digital watermark.

5. The paper medium of claim 4 wherein the digital watermark is embedded on the paper medium using an invisible ink.

6. The paper medium of claim 4 wherein the digital watermark is repeated throughout at least a portion of the paper medium.

7. A printer system comprising:

an image sensor for capturing an image of print media;

a steganographic decoder for reading a steganoraphic message from the image of the print media, the message including printer control information for optimizing printer operation for the print media; and

a printer control unit in communication with the decoder for receiving the printer control information and using the information to optimize printer operation for the print media.

8. The system of claim 7 wherein the image sensor is part of a scanning subsystem in a multifunction device having a printing subsystem and a scanning subsystem.

9. The system of claim 7 wherein the image sensor comprises a CCD array.

10. The system of claim 7 wherein the printer control unit uses the printer control information to look up operating parameters used to control the operation of a printer.

11. The system of claim 7 including a computer connected to a printer; wherein the decoder comprises program code executing on the computer.

12. The system of claim 7 wherein the decoder comprises a watermark decoder.

13. A method for adapting operation of a printer to a type of print media comprising:

capturing an image of at least a portion of a print media;

steganographically decoding a message from the image, including printer control information; and

using the printer control information to adapt operation of the printer to the type of print media.

14. The method of claim 13 wherein steganographically decoding includes decoding the message from a watermark embedded in the print media.

Print Media with Embedded Messages for Controlling Printing

Abstract of the Disclosure

The disclosure describes technology for determining print media attributes and adjusting printer parameters using control data embedded in the print media. In particular, a message embedded in the paper conveys information to the printer about paper characteristics. A printer, or other device with printing capability (e.g., fax machine, scanner, copier, etc.) has a sensor for capturing a representation of the message signal and a decoder for decoding printer control information from the message signal. A control unit in the printer interprets this information and uses it to adjust operation of the printer.

APPENDIX I

MANAGEMENT OF DOCUMENTS AND OTHER OBJECTS USING OPTICAL DEVICES

Related Application Data

The present application is a continuation-in-part of copending applications 09/343,104, filed June 29, 1999, and 09/571,422, filed May 15, 2000.

Field of the Invention

The present invention relates to management of physical objects, including paper documents and computer disks.

Background and Summary of the Invention

The parent applications disclose a document management system that is described, in part, by the following example:

An Excel spreadsheet is printed onto paper, and the paper becomes buried in a stack of clutter on an office worker's desk. Months later the spreadsheet again becomes relevant and is dug out of the stack. Changes need to be made to the data, but the file name has long-since been forgotten. A worker simply holds the dug-out page in front of a camera associated with a desktop computer. A moment later, the electronic version of the file appears on the worker's computer display.

When the page was originally printed, tiny droplets of ink or toner were distributed across the paper in a pattern so light as to be essentially un-noticeable, but which steganographically encoded the page with a plural-bit binary number (e.g., 64 bits). A database (e.g., maintained by the operating system, the Excel program, the printer driver, etc.) stored part of this number (e.g., 24 bits, termed a UID) in association with the path and file name at which the electronic version of the file was stored, the page number within the document, and other useful information (e.g., author of the file, creation date, etc.).

The steganographic encoding of the document, and the updating of the database, can be performed by the software application (e.g., Excel). This option can be selected once by the user and applied thereafter to all printed documents (e.g., by a user selection on an "Options" drop-down menu), or can be presented to the user as part of the Print dialog window and selected (or not) for each print job.

When such a printed page is later presented to the camera, the computer automatically detects the presence of the encoded data on the page, decodes same, consults the database to identify the file name/location/page corresponding to the 24-bit UID data, and opens the identified file to the correct page (e.g., after launching Excel). Voila!

Sometimes there may be several different responses that are possible or appropriate for the encoded object. In the case of a printed office document, for example, one response may be as described

above – to present the electronic version of the file on a computer, ready for editing. But other responses may also be desired, such as writing an email message to the author of the printed document, with the author's email address already specified in the message address field, etc. Various ways of selecting between such options are disclosed.

The parent applications note that such systems can be effected not just with steganographic encoding (e.g., digital watermarks), but other encoding as well – e.g., bar codes.

In the discussion that follows, the present specification expands and enhances the concepts introduced in the parent applications.

Brief Description of the Drawings

Fig. 1 shows an embodiment of a document management system according to one embodiment of the present invention.

Fig. 2 shows a printed document in which embedded hyperlinks are underlined.

Fig. 3 shows portions of a database record associated with the Fig. 2 document.

Detailed Description

In accordance with one embodiment of the invention, a steganographic watermark is added to a document at the time of printing. The printing may be done by a standard office printer (e.g., ink-jet, laser, etc.), or a large clustered on-demand document printer. Each document copy thus contains a mark that can be used to uniquely identify the document. Such marks can be registered in a database and used to link to information about the document.

This functionality can be achieved in various ways. For example, the application program that generated the document (e.g., Microsoft Word or Excel, Adobe Photoshop, etc.) can add the necessary markings to the output data provided to a printer driver. Or the printer driver can perform the function – adding the necessary markings to the output data provided from the application program. A microprocessor within the printer can alternatively perform the function – adding the necessary markings to the data output by the printer driver software. Or this functionality can be performed by various combinations of the foregoing. Etc.

An election to add a watermark to the printed output can be made by the user. This election can be made once, e.g., at the time of printer driver installation, and consistently applied thereafter. Or it can be made on a print-job by print-job or page by page basis, e.g., through a print dialog presented by the application program when the user requests printed output. Or the watermark can be added all the time – without any user election or involvement.

Turning to a particular example, consider the arrangement shown in Fig. 1. An application program 12, such as Microsoft Word or Excel, Adobe Photoshop, etc., sends print data to a software printer driver 14. A watermark data payload that is to be associated with the printed page is either

generated internally by the printer driver, or received from an external input 16. In the depicted system this payload is a 32 bit identifier.

(The length of the payload depends on the application. In some cases, a single bit payload will suffice (e.g., it may serve as a flag to convey a single item of status information about a document – such as confidential, do-not-copy, draft, etc.) Or several such flags may be conveyed by a relatively short payload. Certain textual or numeric information may be literally encoded by the payload, such as the date and time the document was printed (e.g., a 24-bit number representing the number of elapsed minutes since 1/1/2000). The foregoing are examples of direct data encoding. Indirect data encoding, such as the 32 bit identifier cited above, uses the payload as an index into another data repository in which large collections of data can be stored. This collection (sometimes called a "record") may include meta-data associated with the document, such as date, author, size, keywords, file name and storage address, footnotes or other annotations, checksum, etc. In one particular embodiment, identifiers are issued sequentially, with each document thereby assigned a unique identifier.)

By reference to the payload data, the printer driver modifies the print instructions sent to the printer so as to introduce the subtle markings associated with the corresponding steganographic watermark. In some regions of the printed page this entails depositing more ink (or toner); in other regions in may entail depositing less ink. Subtle color variations can also be introduced to effect the encoding.

If the printer driver generates the identifier data itself – rather than receiving the identifier externally – then the identifier will typically need to be stored in a database 18 (or other data structure). Accordingly, the Fig. 1 arrangement shows the printer driver providing the identifier to the database. This database may be stored at a user computer 20, at a remote computer, or may be distributed in some fashion. (If the database 18 is remote from the user computer 20, it would be prudent to encrypt the data transmitted to the database as a security precaution.) Management of the database may be through a dedicated database program (e.g., Microsoft Access), or it can be a simple table data structure or the like maintained by the printer driver itself. (If the identifier data is received externally, this data may be written to the database by the same program that generated or provided the identifier data to the printer driver.)

When, thereafter, the printed document is presented to an optical device, a software program decodes the payload from the steganographic watermark and initiates a corresponding action. If the payload represents status or textual information, the user can be advised of such information (e.g., by a corresponding screen display), or the sensing computer system can take some action based on the information (e.g., refusing to perform a reproduction operation). If the payload represents an identifier, the database 18 is queried for corresponding data, and this data is used in providing a user response. In the case earlier reviewed, the database record contains the file name and storage address of the electronic version of the printed file. The corresponding application program (e.g., Microsoft Word) is then invoked

(if it is not already running), and the identified file is accessed from the specified address and opened. The document is thereby presented on the user's screen – ready for editing.

As with Internet hyperlinks, a problem can arise if a document has been moved from the address associated with that document in the database. One way of managing this is by a software program (which may be termed a daemon) that monitors movements of files within a computer's (or network's) file system, and updates any database records referring to such file locations. Another is for a software program to check all document addresses in the database, e.g., as a background process, to confirm that the referenced document is in the expected location. If a file is not found, the program can undertake an automated search for the file in other locations (e.g., checking file identity by checksum data or the like), and automatically updating database references as appropriate. If files that haven't been accessed for a prolonged period are periodically archived in compressed form on online archival storage, the software program may review recent entries to the archive list and identify the archived location of certain moved files in this fashion. Or the program can simply report missing files to the user so that the user can manually identify a new file location to the database. If a missing file cannot be located, the date of its disappearance can be written into the database record so that, if the document is later needed, the date might be available to help investigate the document's disappearance. Yet another approach that obviates the problem of moved files is to make an archival copy of each file, at the time of printing, in database 18.

In certain applications involving confidential or otherwise secure documents, access to some or all of the stored data may be restricted. In such case, access may be denied unless the user demonstrates suitable authority, e.g., by a password (which may have been earlier entered, such as a network or login password), or by providing some other security token. The token may take the form of biometric identity data, such as voice-print, fingerprint, retinal scan, etc., or may take another form.

In some embodiments, showing the printed document to the optical sensor may cause the computer to present a variety of information, including menu options, to the user. One of the menu options may be to recall the electronic version of the document for editing, as just-described. Other menu options may permit review, or action, based on the associated meta-data.

Increasingly, printed documents include reference to on-line resources – most commonly Internet web pages but sometimes PDF documents, audio or video clips, multi-media presentations, locally-stored files, etc. Microsoft Word and other programs include provision for associating links with text. In Word, this is done by highlighting an excerpt of text, selecting Hyperlink from the Insert menu, and then specifying the path (electronic address) and file (object name) to be associated with that text. Word responds by changing the appearance of the text (e.g., by underlining, and changing color), and embedding the specified link in the electronic version of the document. Such a document is shown in Fig. 2.

When the document is printed, such links can be sensed and stored in a database record associated with that document, and thereafter shown to the user when the printed document is presented to an optical input device.

In one such embodiment, the printer driver monitors print data, looking for text having formatting that is characteristic of an embedded link (e.g., blue text, underlined). Additionally, the printer driver can look for text conforming to standardized addressing protocols (e.g., text beginning with "http://..." or "ftp://..." or "www. ...") When such text is found, the printer driver can store the corresponding link in the database 18 in association with an identifier for that document.

In the case of an explicit address (e.g., "http://..."), the address text itself is copied into the database. In the case of characteristically-formatted text (signifying an embedded link), the printer driver can query the application program that sent the output for printing, to determine the link address associated with each such excerpt of text. These links are stored in the database, together with the text excerpts to which they correspond. (Again, the printer driver inserts at least one steganographic watermark in the printed output – serving to identify the document.) Database excerpts corresponding to the Fig. 2 document, are shown in Fig. 3. (In this example, the document identifier is 186282.)

As in the embodiment detailed earlier, when this printed page is later shown to an optical sensor, decoder software reads a document identifier from the watermark payload and uses the identifier to access one or more database records corresponding to the document. If the record(s) includes one or more links, these can be displayed on the computer screen – available for the user to click and follow. By such arrangement, associated on-line resources are made readily available when reviewing paper documents.

The printer driver's monitoring needn't be limited to on-line resource references. The print data can be monitored for various other types of information, and these other items of information can be stored in the database. One example is document titles, or headings. These can be identified in the printed output by formatting, e.g., set apart from surrounding text by font size, print attribute (bold, underlined, italics), style, or set-apart on a line to themselves -- not ending in a period, etc. If such information is captured at print time and stored in the database 18 in association with the document identifier, the database can serve as an index of sorts to the document contents. The database can later be searched for words or phrases of interest, and documents matching the query can thereby be identified. In some cases, every word in a document (except common noise words) can be logged in a corresponding database record, thereby generating – in real time – an index or table of contents to all documents printed by a given printer or printer driver.

In some applications, the watermark with which the printed document is encoded may be fragile. That is, the watermark may be designed (e.g., by low strength) not to survive expected corruption mechanisms (e.g., the scanning and printing associated with photocopying, compression and decompression associated with JPEG electronic document storage, etc.). If such a mark is not found in a later-encountered document, then the document can be inferred to be a reproduction rather than the original.

Such a frail watermark can be in addition to a robust watermark – one designed to withstand expected corruption mechanisms. Only if both watermarks are detected in scan data from an object is the

object inferred to be an original. Equipment processing the scanned document data can respond differently depending on whether the document is inferred to be an original or a copy, e.g., permitting or disabling certain operations.

In some embodiments it may be desirable for the user to identify himself or herself to the system – preferably in a non-repudiable way (e.g., password or other security token) - when the document is serialized or otherwise assigned an identifier. The database 18 can then log this person's identity in association with that print-out, in case this fact later becomes an issue. Relatedly, it may be desirable for the person who printed the document to specify the intended recipient(s). This data, too, can be stored in the database in association with the identifier that is watermarked in the printed document. If both measures are employed, then when a document is presented to a camera, the responding system can identify both the user who printed the document, and the intended recipient.

Relatedly, digital signature technology can be employed in conjunction with printed documents. As is familiar to those skilled in the art, digital signatures generally involve applying a hash function or the like to a document file, yielding a signature that is stored for later use. If the document file is thereafter changed, even by a single bit, it will no longer yield the same hashed output, or digital signature.

In the present context, the digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark, or can be included in a database record identified by the watermark. If the printed document is thereafter shown to a camera, and an electronic version of the document is retrieved from storage, the signature of the retrieved file can be checked against the signature as represented in the watermark or as stored in the database record. If the signatures don't match, the electronic version of the document is known to have been altered.

Checksums derived from the electronic version of a document can be used in similar fashion to digital signatures.

Still another option is to encrypt an electronic version of a file, and encode an encoding key in a watermark in the printed document (or in a database record identified by the watermark). The person who encrypted the document knows the key and can open the electronic file. But third parties cannot open the electronic version of the document, unless they have custody of a printed version of the document. (This is an application where a fragile watermark would be beneficial, so that custody of a photocopy would not be sufficient to gain access to the electronic file.)

Similarly, printed documents may convey (or may point to database records containing) encryption keys permitting electronic access to unrelated documents.

It will be recognized that public key encryption, as well as private key encryption, can be used in certain of the foregoing contexts.

Techniques like those reviewed above in connection with office document can be applied to other objects as well. A "document" can thus be any object with printing, such as packaging.

Consider a catalog for a data storage medium, such as a diskette, disk, tape, CD, or DVD. Files can be copied onto the medium, and an electronic directory listing can be generated (e.g., by using the DIR function of DOS, or the counterpart functions provided in Microsoft Windows and other operating systems). If desired, the directory listing can be annotated by a user, e.g., by adding descriptive information.

This listing is stored in a data structure (e.g., a table, database, etc.) in association with index data. This index data is encoded in a watermark or other machine-readable indicia and printed on a label that is applied to the medium. (Additional data can also be printed on the label in human-intelligible form, such a text giving the date the diskette was labeled, the proprietor of the disk, a descriptive name or summary of disk contents, etc.)

By holding such a labeled disk to a webcam, video camera, optical mouse, or other optical input device, a listing of the disk's contents can rapidly be displayed. (As is now familiar, the optical input device provides image data corresponding to the label to a watermark detector. The watermark payload that is output from the watermark detector is used to index the data structure, permitting access to the corresponding directory listing. This listing is then presented on the computer screen for display.)

The user may be invited to specify certain search parameters, such as author, file date, file name, etc. Only files in the directory listing meeting the specified criteria can then be displayed. If a particular file name is specified, the user can hold diskettes up to the webcam in rapid succession, permitting dozens of diskettes to be surveyed in a minute or so, looking for the desired diskette.

The display presented to the user may include content listings of a collection of disks – not just the disk presented to the webcam. For example, presentation of a 3¼ inch diskette to the webcam may prompt a listing of all 3¼ inch diskette contents contained in the data structure, or all such disks labeled on the same date as the diskette presented by the user to the webcam (in both cases, with the contents of the user-presented diskette listed first). If the file sought is not cataloged as being on the first-listed diskette list, a Search or Find function can be executed on the listing to identify another diskette on which a desired file is stored. (The identification of like-media can be effected by selecting index identifiers from different ranges for different media. Thus 3¼ inch diskettes may have identifiers in one range, CDs may have identifiers in another, etc.)

The data structure may be posted to a shared resource on a network, so that this functionality can be effected on an enterprise-wide basis, encompassing large collections of files stored on diverse media.

The arrangement just detailed can be adapted for use in other contexts, to provide electronic listing of data associated with diverse physical objects

From the foregoing, it will be recognized that embodiments according to the present invention permit data about an object to be accessed simply by showing the object to a webcam or the like.

Having described and illustrated the principles of the invention with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while the detailed embodiments were described as employing steganographic digital watermarks, the same principles can likewise be utilized in conjunction with other marking techniques, including 1D and 2D bar codes, data glyphs, OCR, magnetic ink, etc.

Essentially any digital watermarking technology can be used in the described embodiments. One particular technology is detailed in the present assignee's patent application 09/503,881, filed February 14, 2000, and in other references cited herein. Those skilled in the watermarking art are familiar with a great number of particular watermarking techniques.

In some cases, printing is not required to effect a digital watermark. For example, the watermarking can be effected by texturing, e.g., as disclosed in the present assignee's patent 5,822,436.

While the invention was particularly described with reference to an implementation involving a Windows printer driver, other forms of implementation are possible. Consider, for example, Adobe Postscript – a popular page description language implemented in many office printers. Watermarking may be included as an intrinsic feature of a Postscript printer engine (or any page description lanaguage). As part of printing a document, any embedded links could be registered in a suitable database 18, and the printing commands could be modified to include the appropriate ID with the setup for each page. Addition of a tint to effect watermarking could be provided when the document is converted by the engine from text to ink/toner/dye. A further advantage here is that the printer itself could have certain meta-data associated with it that is conveyed in the watermark or stored in a database record to which the watermark points (e.g., data specifying that the document was printed on a HP LaserJet 8000, with a network name of "XYZ," having port address of \\Cobra\LGL-HP8000, from a print job originated by user BCONWELL, etc., etc.). And the embedding process may be tuned by the vendor implementing the Postscript engine on their platform for optimal performance.

The illustration of the invention in the context of office documents and diskettes should not be taken as limiting its utility. To name but one other application, blueprints and other construction drawings can be encoded with a watermark. Again, the watermark can directly encode meta data, or can point to a data structure where such further information is stored.

One of many applications of such information is to ensure that a contractor is working from the latest revision of a drawing. A camera-equipped cell phone, or wireless palmtop computer with imaging capability, can be used by the contractor to acquire image data from the drawing, decode the embedded watermark ID, query a remote database for the latest revision number of that drawing, and present the latest revision number to the contractor. The contractor can check the number thus-obtained with the revision number printed in the title block of the drawing. If they match, the contractor is assured that the drawing depicts the latest information. (Blueprints and construction diagrams are forgiving media – the watermark needn't be invisible. The strength of the watermark can thus be increased to the point that a pebbling or grainy effect appears on the background of a drawing without reducing the drawing's functionality for its intended use.)

While the invention was described with reference to certain functionality implemented in software, this is not essential. Hardware, of a combination of hardware and software can be used in other embodiments. Likewise, the form of optical detector is not crucial. 2D sensor arrays, such as CCD and CMOS cameras (still or video) can be employed. So, too, can 1D sensor arrays, such as are conventionally found in scanners. Single photosensor systems, such as laser diodes with photodiodes can also be used.

The foregoing techniques can be employed in conjunction with teachings of various of the present assignee's co-pending applications, including 09/074,034 (filed May 6, 1998), 09/127,502 (filed July 31, 1998), 09/185,380 (filed November 3, 1998), and the parent application cited above. For example, the '034 and '502 applications disclose arrangements for watermarking blank paper stock, the principles of which can be employed to mark printed output.

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the patents and applications cited above.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

WE CLAIM:

1. A method for opening a file on a computer system, comprising presenting a printed version of said file to an optical sensor.

2. A method comprising:

presenting a printed document to an optical sensor; and

in response thereto, loading an electronic version of said document using an application program with which the document was originally generated.

3. A method of electronic management of paper documents, comprising:

presenting a paper sheet to an optical sensor, the paper sheet having an optically-detectable indicia thereon, said indicia being machine-readable, but not generally intelligible to human viewers thereof, the optical sensor producing scan data;

decoding the scan data to produce binary data corresponding to said indicia;

accessing a data store using at least a portion of said binary data; and

obtaining from said data store an electronic address at which an electronic version of said paper document is stored.

4. The method of claim 3 that further includes:

determining an application program suitable for opening said electronic version;

opening said electronic version with said application program; and

displaying said electronic version on a computer screen.

5. The method of claim 3 wherein the indicia is a steganographic watermark.

6. The method of claim 3 wherein the indicia is formed by ink-jet printing.

7. The method of claim 3 wherein the electronic address was stored in said data store at the time said paper document was printed.

8. The method of claim 3 wherein the optical sensor comprises an array of plural image photosensor elements.

9. A method of producing a printed document from document data provided by an application program, the method including using a printer to apply ink or toner to a substrate, the method being characterized by adding data corresponding to an optically-detectable indicia in print data corresponding

to said document data, said indicia being machine-readable, but not generally intelligible to human viewers thereof, said indicia encoding plural bits of digital data.

10. The method of claim 9 in which said adding is performed by printer driver software.

11. The method of claim 10 in which a print dialog interface associated with said printer driver software gives a user thereof an option to elect formation of said indicia on the printed document, or not.

12. The method of claim 9 in which said adding is performed by hardware or software resident in the printer.

13. The method of claim 9 wherein the indicia comprises a steganographic digital watermark.

14. The method of claim 9 wherein said digital data includes an identifier corresponding to a database record, the method further including storing data relating to the printed document in said database record.

15. The method of claim 14 that includes transmitting said data for storage in the database record in encrypted form.

16. The method of claim 9 wherein said digital data encodes meta data relating to the document.

17. A printed document produced according to the method of claim 9.

18. A method of printing a document using print data output from an application program, comprising:

monitoring the print data for text associated with a hyperlink;

storing information about said hyperlink in a data structure, in association with a document identifier; and

printing the document with an optically-detectable indicia thereon, said indicia being machine-readable, but not generally intelligible to human viewers thereof, said indicia representing a plural-symbol payload including said document identifier.

19. A printed document produced according to the method of claim 18.

20. A method comprising:

presenting a printed document to an optical input device; and

presenting to a user one or more electronically actuable hyperlinks included in said printed document.

21. A method comprising:

monitoring print data sent from an application program to a printing system, to detect text of a certain class; and

storing, in a database, information relating to such text detected in the print data.

22. The method of claim 21 in which the text is selected from the group consisting of one or more of the following classes: references to on-line resources, titles, and headings.

23. A printer including a page description language engine, the engine serving to add machine readable indicia to printed output produced by said printer, said indicia being generally unintelligible to human viewers, but conveying plural bits of digital data.

24. A method comprising:

capturing image data from at least a portion of a blueprint or construction diagram;

decoding an identifier from a machine readable indicia represented in said image data;

transmitting said identifier to a database;

accessing a database record corresponding to said identifier and obtaining from said record certain revision data relating to said diagram; and

transmitting said revision data to a user.

25. The method of claim 24 wherein the transmitting includes at least one wireless transmission.

26. A method for determining the contents of one or more computer data storage media, comprising presenting such media to a camera.

MANAGEMENT OF DOCUMENTS AND OTHER OBJECTS USING OPTICAL DEVICES

Abstract of the Disclosure

By printing documents and other objects with machine readable indicia, such as steganographic digital watermarks or barcodes, a great variety of document management functions can be enabled. The indicia can be added as part of the printing process (after document data has been output by an originating application program), such as by printer driver software, by a Postscript engine in a printer, etc. The indicia can encode data about the document, or can encode an identifier that references a database record containing such data. By showing the printed document to a computer device with a suitable optical input device (e.g., a webcam), an electronic version of the document can be recalled for editing, or other responsive action can be taken.

APPENDIX J

LINKING FROM PAPER INVOICES AND STATEMENTS TO ON-LINE RESOURCES

Field of the Invention

The present invention relates to invoices, bank statements, and other account paperwork that is exchanged between parties in connection with commercial transactions, and more particularly relates to the integration of such paperwork with on-line systems.

Detailed Description

In application 09/571,422, filed May 15, 2000, the present assignee disclosed various arrangements for linking from physical objects (e.g., business cards, milk cartons, etc.), to associated on-line resources. The physical objects can be marked with steganographic digital watermarks (e.g., as detailed in application 09/503,881, filed February 14, 2000), or by other machine-readable indicia such as bar-codes, data glyphs, etc.

In accordance with the present invention, these same principles are applied to invoices, bank statements, and similar account paperwork.

More particularly, such paperwork includes indicia that encodes information corresponding to an on-line address. When the indicia is sensed by a corresponding sensor (e.g., a web cam), the address information is decoded, and a link is established between the user's computer and the corresponding on-line address. Most commonly, the encoded information is an identifier that is used to index a database record containing the on-line address. This address is then provided to an Internet browser on the user's computer, permitting a corresponding web page to be loaded. In other embodiments, the on-line address can be directly encoded in the indicia.

In the case of a utility bill or the like, a consumer shows the bill to the web cam. (The bill can be held in front of the camera, or the camera can be held over the bill.) Browser software on the consumer's computer responds an instant later with a web page customized to that user, including an electronic version of the bill. A user interface included on the web page permits the consumer to authorize electronic payment of some or all of the amount due, either by credit card, electronic funds transfer from a bank account, or otherwise. Account review (both current and historical), customer service, and related services can also be provided via the web page. The web page may also include third party targeted advertising, as well as promotional information provided by the billing company (e.g., a cable company may use such web sites to inform customers of upcoming events, a telephone company may use the sites to promote special offers, etc.)

In addition to on-line payment, such a web page may provide for printing of a corresponding paper check at the user's computer – with the payee, amount, and date fields filled in automatically so as to

prevent transcription errors. This functionality may be provided by a linkage between the web data and check-writing features of programs such as Microsoft Money or Quicken. Or the web page can include an embedded aplet that directly prints a corresponding check from the user's computer, etc. Regardless of payment technique, the system can update the user's corresponding account information accordingly (e.g., entering an electronic payment in an on-line check register).

Such an arrangement offers the best of the print and electronic worlds. For the customer, it reduces the time to pay bills, and avoids the time and expense associated with writing and mailing checks. Payments can be controlled by the customer to meet their particular needs (e.g., scheduling of payments, making partial payments). The system is simple – just show the paper invoice to the computer. And the system is failsafe, in that if the electronic network goes down, the user can write a check based on the paper invoice, as always.

For the billing business, the system reduces administration costs by reducing physical mail and check processing, while providing enhances customer service. And the provision of targeted advertising provides a further revenue opportunity.

and provides enhanced customer service.

Much the same arrangement can be used with bank statements - for checking accounts and the like. The paper statement mailed to the customer is digitally watermarked, permitting an on-line version of the statement to be accessed simply by showing the paper to a web cam. Customary on-line banking tools can be included at the web site, including interfaces with common on-line banking software such as Microsoft Money and Quicken. (Indeed, the watermark reader may be included as an element of such software, or as an auxiliary utility that cooperates with the on-line banking software.)

Likewise, checks can be digitally watermarked – both checks printed by commercial check printers, and checks printed on home computers using various home banking software. The watermark can uniquely identify the check. When such a check is presented to a webcam, associated software can link to a database to obtain, and display, information relating to the check. The database can be on a remote computer (e.g., the bank's computer), or can be local (e.g., a check register maintained on by a home computer software application, such as Microsoft Money, or Quicken).

In all such approaches, a generally increased level of security is inherent, since the system relies on custody of the physical invoice or bank statement to gain access to the web page – a circumstance that imposters will find difficult to imitate. This circumstance notwithstanding, the web page may also include password protection or other security measures to guard against unauthorized access, e.g., from discarded account paperwork. (Account paperwork older than a set threshold, e.g., 45 days, may be disabled from access, if desired, to help protect against unauthorized use.)

To provide a comprehensive disclosure without unduly lengthening this specification, applicant incorporates by reference the patent applications cited above.

Having described and illustrated the principles of my invention with reference to specific

embodiments, it will be recognized that the principles thereof can be implemented in many other, different, forms.

For example, while the detailed description contemplated use in conjunction with a web cam and personal computer, a great variety of other platforms can also be employed. These include set top boxes, smart phones, palm computers and organizers, etc. – any of which can provide Internet linking.

Likewise, while the detailed description particularly contemplated use of digital watermark technology, some of the same advantages can be achieved through use of other machine readable indicia, including bar codes, data glyphs, etc.

Moreover, the particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with teachings in the incorporated-by-reference applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, I claim as my invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

I CLAIM:

1. An on-line method of paying funds from a first party to a second party in accordance with a statement detailing an amount owed, comprising:

the first party receiving said statement, on paper, by conventional mail;

the first party presenting at least a portion of said paper to an optical sensor; and

processing data from said optical sensor, including displaying a page of electronic information related to said statement on a screen of a data terminal.

2. The method of claim 1 wherein said page of electronic information permits the first party to authorize electronic disbursement of said funds to said second party.

3. The method of claim 1 that further includes printing a check on a printer associated with the first party, for payment of said statement, without manually entering the payee on the check.

4. The method of claim 1 wherein the statement becomes ineffective in leading to said page of electronic information after the passage of a predetermined period, so as to prevent discarded statements from being used by unauthorized persons to gain access to said page of electronic information.

5. A computer storage medium having instructions thereon causing a computer to perform the processing of claim 1.

6. A method for accessing on-line account information corresponding to a bank or other commercial account, comprising presenting a printed account statement, received by conventional mail, to an optical sensor.

7. A method comprising:

presenting a printed account statement, received by conventional mail, to an optical sensor; and

in response thereto, loading an Internet web page having electronic information corresponding to said account.

8. The method of claim 7 wherein the account is a utility account.

9. The method of claim 7 wherein the account is a bank account.

10. An invoice having a machine readable indicia thereon, said indicia representing plural bits of

binary data, said indicia being generally un-intelligible to human observers thereof, the binary data represented by said indicia serving to indicate an on-line computer address associated with said invoice.

11. The invoice of claim 10 wherein the indicia includes an identifier that is associated with said on-line computer address through a database record.

12. The invoice of claim 10 wherein the binary data represents said on-line computer address.

13. The invoice of claim 10 wherein said indicia comprises a steganographic digital watermark.

14. The invoice of claim 10 wherein said indicia comprises a barcode.

15. A checking account statement having a machine readable indicia thereon, said indicia representing plural bits of binary data, said indicia being generally un-intelligible to human observers thereof, the binary data represented by said indicia serving to indicate an on-line computer address associated with said checking account statement.

16. A printed check having a steganographic digital watermark encoded thereon, said watermark representing plural bits of binary data, the binary data represented by said watermark serving to indicate an on-line computer address associated with said check.

17. A computer storage medium having an electronic checkbook software program stored thereon, wherein said program incorporates, or cooperates with, software instructions that process image data to extract a steganographically-encode watermark payload therefrom.

LINKING FROM PAPER INVOICES AND STATEMENTS TO ON-LINE RESOURCES

Abstract of the Disclosure

Invoices, bank statements, checks, and other transactional paperwork is encoded with a steganographic digital watermark that encodes identification information. When a user shows such a paper (e.g., an invoice) to an optical input device associated with a computer, a browser session is initiated that uses the identification information to transport the user to a web page corresponding to that invoice. The web page provides a variety of functionality, including account review and payment, and customer service.

APPENDIX K

PRINTING MEDIA AND METHODS EMPLOYING DIGITAL WATERMARKS

Related Application Data

This application is a continuation-in-part of copending application 09/567,405, filed May 8, 2000.

Other related applications are cited below in connection with particular teachings for which they are relevant.

Field of the Invention

The present invention relates to use of digital watermark technology in conjunction with envelopes and other documents.

Background and Summary of the Invention

Computer printers have long been used to print addresses on envelopes. With the advent of digital postage, use of printers with envelopes is increasing still further.

Digital postage technology is available from a number of vendors including Pitney Bowes, E-Stamp, Stamps.com and Escher Laboratories (of Escher Group, Ltd.), and is detailed in various patent publications including 5,982,506, 5,825,893, 5,819,240, 5,801,364, 5,774,886, 5,682,318, 5,978,781, and WO 99/18543A1.

Digital watermarking technology is used, in accordance with certain embodiments of the present invention, to increase the security of, and augment the functionality associated with, computer printing of envelopes and postage.

In accordance with one aspect of the invention, traceability of digital postage is enhanced by serialization, i.e., embedding a serial number code or other indicia that uniquely and covertly links the printed postage to some device or software in the users' possession, or that identifies the user. This device can be a printer, personal computer, or hardware security device used in printing the postage. In an exemplary embodiment, digital watermarking of the sort detailed in the cited patents and applications is used to embed the code at the time the postage is printed. The embedded data would only be detectable to investigators equipped with special readers for spot checking documents or investigating counterfeits.

In accordance with another aspect of the invention, security of digital postage against reproduction is enhanced through use of "fragile" digital watermarks. (A "fragile" digital watermark is one designed, e.g., not to fully withstand the scanning/printing operations associated with photocopying or PC-based scanning and printing.) Such a watermark may be employed to provide forensic evidence that printed postage is not original.

In accordance with yet another aspect of the invention, watermark technology is employed to prevent – outright – the photocopying or other duplication of digital postage. This result is achieved by encoding on envelopes a "do not copy" watermark to which photocopiers, scanners, printers, and other

computer devices are alert. If such a watermark is encountered, the device will refuse to operate, or will otherwise interfere with the reproduction operation.

In accordance with still another aspect of the invention, watermarking on an envelope is employed as an element of a franking mark (postal mark) – one that may stay within or extend well beyond the corner location typically associated with such marks.

In accordance with yet another aspect of the invention, watermarking on an envelope can serve as a portal to a corresponding internet site or internet-based application. That is, a printed document with an embedded watermark can be held up to a web cam, or scanned by a scanner, and instantly link a user to Internet sites or applications. Importantly, information received in this manner is not subject to the delays associated with physical mail delivery, but can convey up-to-the-minute information.

In accordance with still another aspect of the invention, an envelope watermark serves to convey an identifier that is used to access associated data in a database. In one particular application, the index number identifies the recipient. Thus, for example, an envelope can be addressed simply by watermarking it with a unique recipient designator, e.g., JOHNQPUBLIC843. Processing equipment in the postal system can read the watermark, query a database with the designator, and determine thereby the recipient's physical address. (If desired, the address thereby discerned can be printed on the envelope.) One advantage to this arrangement is that distribution of Change of Address cards would be a thing of the past. If a person moves across country, a single record in the database is changed. All mail to that recipient automatically is directed to the new physical address.

In accordance with yet another embodiment, digital watermarks on envelopes can be applied by specialized printers (e.g., postal metering devices), or by using common office printers (e.g., laser, ink-jet). In such systems, the watermark embedder software may be integrated into the printing device, or can be resident on an associated computer system. The software is desirably secured against tampering using various anti-hacking techniques. The production of the digital watermark may not be optional (i.e., it may be applied without user control), and the payload can be tailored in accordance with the amount of postage, device/software/user information, or other application information. Such a system may also include an application that calibrates printing of the watermark to the user's specific printer or software, thus accommodating a wide range of usage scenarios. A hardware security device used, e.g., to store postage value (e.g., a digital vault) may also be employed by the watermark embedding system, e.g., as a source of secure and potentially unique data used in encoding the digital watermark.

In accordance with still further embodiments of the invention, the principles described herein are also applicable to other printed value documents (e.g., tickets and coupons), especially those that are printed on demand. Such documents may be printed at home, at special kiosks (e.g., in-store), or by commercial printing establishments (i.e., mass produced). Among other functionality, the watermarks in such value documents can be used by investigators to distinguish originals from reproductions (by use of fragile watermarks), to authenticate documents (e.g., in ticket reading machines), and to link to associated

internet resources. The watermarks can also be linked to other information (e.g., event date, seat number, product code, etc.) textually printed on the document, or present on the document in some machine readable form (e.g., barcodes). In such case, the watermark can be used to detect document alteration by checking for discrepancy between the watermark-encoded information, and that otherwise conveyed by the document.

In accordance with yet other embodiments of the invention, blank printing stock (e.g., other than envelopes) can be digitally watermarked to serve various ends. The watermarking continues to be detectable after the blank stock is thereafter printed.

The features just-described can be employed alone or in various combinations.

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description.

Detailed Description

Digital watermarking technology, a form of steganography, encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration or data representation.

Digital watermarking of envelopes can be effected in numerous ways, including by ink (clear, optically-opaque, IR/UV-opaque), by texturing, by laminate layers, etc. The watermarking can be formed as part of other markings on the envelope (e.g., franking marks, graphics, text, etc.), or can be applied irrespective of such other markings. Watermarking can be effected at any time in an envelope's life, including at the time of media-making (e.g., paper making or Tyvek formation), at the time of envelope making, at the time of consumer use (either before, during, or after the application of other envelope markings), and thereafter (e.g., in the course of postal service processing).

The watermarking may span all of one side (or both sides) of an envelope, or may be localized, e.g., in the areas typically associated with postage, return address, and recipient address. An envelope may convey a single watermark, or several may be used, e.g., conveying different information or serving different purposes in different regions. Several different watermarking technologies can be employed on a single envelope, e.g., the envelope's texture can convey one type of information, and tinting printed on the envelope can convey a second type of information.

Any print- or physical media-watermark technology can be employed in conjunction with the present invention. Representative watermarking technologies suitable for such use are detailed in the assignee's patent 5,862,260, and in applications 09/074,034, 09/127,502, 09/503,881, 09/562,516, and 09/562,524. A great many other watermarking technologies are familiar to those skilled in the digital watermarking art.

In accordance with one aspect of the invention, traceability of digital postage is enhanced by serialization, i.e., embedding a serial number code or other indicia that uniquely and covertly links the printed postage to some device in the users' possession.

In one such embodiment, the watermark serves to convey an identifier of a printer, personal computer, postage vault, or other device used in printing postage. The identifier can be a registration number, a serial number, an account number, etc. The watermark can also serve to convey an identifier associated with particular software employed by the user. And/or, the watermark can also serve to identify the user. Other forensic information can likewise be encoded.

The encoded information can directly correspond to the device, etc., or the relationship can be established through a remote database (e.g., the identifier can be an index number that, when looked-up in a database, yields the registered owner name and address of a particular device).

Typically, such a watermark is "private," i.e., it is readable only to selected classes of persons who have access to secret data, such as a private key. Postal investigators and the like would be able to read such data (e.g., by using a specialized reader system, or by using a conventional reader system equipped with the private information), but the general public would not.

In other embodiments, the watermark is public, but general use thereof is limited because a database needed to interpret the encoded data is not publicly accessible.

As indicated above, this forensic watermark can take various forms. For example, it can form part of the franking indicia printed on the envelope, or can be separate from such indicia. It can be limited to the franking corner of the envelope, or can be located in a different location, or span a larger area. One particular implementation deposits a light splattering of tiny ink droplets over an area. These droplets are sufficient to form a computer-detectable pattern, but are not conspicuous (or preferably even visible) to human observers. In this, and other embodiments, the invisibility of the markings can be enhanced by using inks responsive to ultraviolet or infrared illumination, as more particularly detailed in cited application 09/562,516.

In most applications, the forensic watermark is applied automatically as part of another envelope processing activity. Thus, for example, such functionality can be provided in software used to print addresses on envelopes, or apply digital postage to envelopes. The software can be of the consumer variety (e.g., Microsoft Word), or it can be system or device instructions invoked as part of the printing operation (e.g., printer driver software, or firmware associated with a printer's microprocessor.) As the user-intended information is being printed, the forensic marking is also being applied. Thereafter, if an issue arises as to the source of an envelope, or postal indicia thereon, the forensic information can be checked to aid in such investigation.

In accordance with a second aspect of the invention, security of digital postage against reproduction is enhanced through use of "fragile" digital watermarks.

As noted, a "fragile" digital watermark is one designed not to fully withstand the scanning/printing operations associated with photocopying. (The use of fragile watermarks is detailed in the assignee's applications 09/234,780, 09/287,940, 09/433,104 and 09/498,223, 09/625,577, 60/198,138, 09/645,779, and in three applications filed herewith: Halftone Watermarking and Related Applications

<docket 60302>; Watermarks Carrying Content Dependent Signal Metrics for Detecting and Characterizing Signal Alteration <docket 60305>; and Watermarking Recursive Hashes Into Frequency Domain Regions <docket 60306>.) If markings (e.g., legitimate franking indicia) incorporating such a watermark are photocopied or otherwise reproduced from one envelope onto a second envelope, the copy will either not fully include the watermark, or the watermark will be changed in a way that indicates it is a copy. Processing equipment in the postal system can be alert to such copies (which are identified by the absence or modification of the fragile watermark), and cull them from the properly-franked mail. Likewise, fraud or counterfeit investigators can use special readers to verify originality and detect copies.

A watermark may be made fragile in numerous ways. One form of fragility relies on low watermark amplitude. That is, the strength of the watermark is only marginally above the minimum needed for detection. If any significant fraction of the signal is lost, as typically occurs in photocopying operations, the watermark becomes unreadable.

Another form of fragility relies on the watermark's frequency spectrum. High frequencies are typically attenuated in the various sampling operations associated with digital scanning and printing. Even a high amplitude watermark signal can be significantly impaired, and rendered unreadable, by such photocopying operations.

The foregoing are but two of many different approaches. The above-cited applications disclose many others. The particular fragile watermark used can be tailored in accordance with the type of scanning and printing anticipated in unauthorized reproduction.

Likewise, the fragile watermark can be implemented in various ways. For example, the watermark can be implemented by varying thicknesses of lines, adding dots or speckles or ink, or modulating the brightness of printed pixels. (Such watermarking arrangements are further detailed in applications 09/074,034 and 09/127,502.) Or the watermark can be formed by texturing of the substrate. Such texturing can be applied in various ways. One is by a mechanism integrated with the printer, e.g., one that impresses the medium with a pinch roller or other pressure-applying means. Another is during fabrication of the paper, e.g., by texturing dewatering elements in the paper making machinery to impress a desired pattern on the medium. (One such arrangement is detailed in application 09/437,357, filed November 10, 1999.)

As indicated, processing equipment in the postal system (e.g., document sorters and postal processing machines) can routinely scan envelopes bearing digital postage for the presence of the expected fragile watermark. Any envelopes found to be missing the watermark can be culled for investigation. This analysis may include watermark-reading software that infers information about the type of reproduction employed by reference to the attributes of any remaining fragile watermark signal.

In accordance with a third aspect of the invention, watermark technology is employed to prevent – outright – the photocopying or other duplication of digital postage. This result is achieved by encoding on envelopes a "do not copy" watermark to which photocopiers, scanners, printers, imaging software, or

other computer devices are alert. If such a watermark is encountered, the device will refuse to operate, or will otherwise interfere with the reproduction operation.

Such watermark-based "do not copy" systems are further detailed in applications 09/074,034, 09/127,502, 09/185,380 and 09/287,940. The detection of the watermark can occur in various, and preferably numerous, locations in likely reproduction systems. In a desktop computer system, for example, image data may be analyzed for such a watermark by software in the scanner (e.g., scanner driver software), software in the computer (e.g., TWAIN interface software, operating system software, image editing software, internet browser software, printer driver software), and software in the printer (e.g., printer firmware). If any of these detectors encounters image data that has a "do not copy" watermark encoded therein, the detector will interfere with its reproduction (e.g., by discontinuing the process, by scarring the image, by hiding tracer data for later forensic use, etc.)

The use of a watermark to indicate that an indicia should not be copied is desirable, but not necessary. Other hallmarks can be employed. For example, devices used in reproduction can be alert to the franking indicia itself and, if encountered, interfere with duplication.

In accordance with a fourth aspect of the invention, security is enhanced by associating (cryptographically or otherwise) a digital watermark formed on envelope stock (e.g., by printing or texturing) with data conveyed in a postal franking mark (e.g., a 2D bar code). In such case, for example, the envelope can be authorized for use only in conjunction with a certain printer, a certain postal meter, a certain postal account, a certain software, etc. If the envelope stock is diverted to another use (e.g., used in conjunction with a different postal meter), the discrepancy in the association between the envelope watermark and the postal franking mark can be detected by the postal authorities, and suitable action taken (e.g., alerting the proper owner of the envelope stock of such use).

The association between the envelope watermark and the postal indicia can be self-contained (e.g., the association can be demonstrated without reference to external resources), or a remote resource can be employed (e.g., a database can specify that envelope stock X should only be encountered with digital postage from account Y).

In a variant embodiment, a franking station can check the watermark already existing on an envelope prior to applying postage. If a correct watermark is not detected, the franking station can decline to apply postage absent supervisory clearance. Unauthorized use of corporate mail accounts for use on personal correspondence may thereby be curbed.

In accordance with a fifth aspect of the invention, watermarking on an envelope is employed as an element of a franking mark. Such marking can be confined to the corner location typically associated with postage, but need not be so limited. If the marking extends across the entire envelope – on one side or both – machine processing of the mail by the postal system can be facilitated by obviating the need for positioning the envelope in a certain orientation for reading. In one particular embodiment, an embedded calibration signal associated with certain watermarks (c.f., the cited patent documents) can be used to

orient a digital image of the envelope for both watermark reading as well as for other machine processing. In other embodiments, printed features of a franking mark (e.g., vertical and horizontal lines) can be used like graticules to aid in establishing the skew of a watermark printed with the franking mark, thereby aiding decoding of the watermark.

To make clear to office personnel that postage has been applied to such an envelope, it is generally desirable that the marking be visible. This can be achieved by increasing the amplitude of the watermark signal so that it appears as a patterned tile (or other shape). Or the watermark can be imperceptible, and other indicia added to indicate that postage has been applied (e.g., text stating "Posted with $0.33, printed in the same area as the watermark, or in a different area).

In still other arrangements, a conventional 2D barcode franking mark is subtly changed to, itself, imperceptibly carry the watermark.

The information encoded in the franking (or other) watermark can represent a great variety of data. The amount of postage encoded, the date of encoding, the sender's name, address and zip code, the recipient's name, address and zip code, etc., can all be indicated.

In some embodiments, all such information is directly encoded in the watermark. In other embodiments, the watermark encodes an abbreviated data set, e.g., including a code number. The code number corresponds to additional information that can be found in a database record accessed by the code – either maintained by the user, by a central authority (e.g., the postal system), or by some remotely accessible database.

In accordance with a sixth aspect of the invention, watermarking on an envelope serves as a portal to a corresponding internet site or application (which could be local on the user's PC).

As detailed in the assignee's application 09/571,422, filed May 15, 2000, a watermarked document can be held up to a web cam, or scanned by a scanner, and serve to instantly link a user to an Internet site, to invoke an application, etc. (The present assignee offers such services under the Digimarc MediaBridge name.) An envelope marked in this fashion can allow a user to initiate an essentially unlimited range of options.

Consider an envelope having the sender's contact information (name, address, zip code, phone number, fax number, email address, etc.) represented by a watermark (either literally, or referring to a database record). A recipient of the envelope may present same to a web cam associated with a personal computer. The camera decodes the watermark, finds it is contact information for a person, and in response automatically adds the contact information to a contact organizer (e.g., Microsoft Outlook) maintained by the computer.

Different watermarks may trigger different reactions. Certain of the payload bits in the watermark may indicate the type of data represented, and/or the type of reaction that is appropriate. Responses may be programmed by the sender, so the watermark is the same, but the backend system that is linked to the watermark contains the programming for what response to invoke.

One type of watermark may indicate that the encoded information is contact information that is available for loading into a recipient's contact organizer. A second type of watermark may indicate that a delivery confirmation message is to be dispatched to the sender of the envelope. When such an envelope is presented to the receipient's web cam, the associated computer automatically composes an email message confirming delivery of the envelope, and sends it to an address represented in the watermark.

A third type of watermark may direct a web browser associated with the recipient's computer to a destination specified by the watermark. The destination web address can provide the recipient with additional information related to the mailing, but updated to the minute. Advertising mailings can thus link to ordering pages, new sale promotions, updated backorder status information, etc. Utility bills can link to summary account information showing payments received or owing, month-to-date charges, etc. The linked web address may present a form soliciting input or response from the envelope recipient, including survey responses, votes, etc.

The linked resource needn't convey just textual or graphical information. Entertainment programming can be similarly invoked, e.g., the delivery of previews of tonight's cable television shows, popular music recordings for preview or purchase, etc.

A fourth type of watermark may initiate a replenishment of postage in the recipient's digital postage account.

The foregoing is just a small sampling of the myriad functions that can be invoked – locally in the recipient's computer, or employing remote resources (e.g., computers accessed over the internet) – in response to presentation of a mailing to a webcam or other imaging device.

Some watermarks may correspond to several alternative actions. In such case, the recipient's computer may present a menu from which the recipient can select the desired response. Or the response invoked by presenting the envelope to the web cam may be made dependent on context or environment in which the presentation is made (e.g., time of day, type of device to which web cam is connected – fixed or portable computer, wired or wireless, etc.)

In a variant of the foregoing embodiment, an envelope watermark serves to convey an identifier that is used to access a database record having information related to mail processing or delivery. In one particular application, the index number identifies the recipient. Thus, for example, an envelope can be addressed simply by watermarking it with a unique recipient designator, e.g., JOHNQPUBLIC843. Processing equipment in the postal system can read the watermark, query a database with the designator, and determine thereby the recipient's physical address (e.g., street address).

In some such embodiments, the physical address information obtained by this database lookup is printed on the envelope by the postal system for the benefit of the ultimate postal delivery person. In other embodiments, the postal delivery person is equipped with reader devices that make such printing superfluous.

As noted, an important advantage to this arrangement is that Change of Address cards would be a thing of the past. If a person moves across country, a single record in the database is changed. All mail to that recipient automatically is directed to the new physical address. A lifetime postal addressing system can thereby be realized.

In accordance with yet another embodiment, digital watermarks on envelopes can be applied by postal metering devices, or by using common office printers (e.g., laser, ink-jet). In such systems, the watermark embedding functionality may be integrated into the printing device (e.g., by firmware executed by a printer microprocessor, or by dedicated hardware), or can be resident as software on an associated computer system. The software is desirably secured against tampering using various anti-hacking techniques. The production of the digital watermark may not be optional (i.e., it may be applied without user control), and the payload can be tailored in accordance with the amount of postage, device/software/user information, or other application information.

Such a system may also include an application that calibrates printing of the watermark to the user's specific printer or software. For example, the application (which may be a software program) may print a predetermined pattern (watermark or otherwise). The resulting printed media can then be scanned using a scanner (e.g., a digital photocopier or other device) whose transfer function is known. (The application may have profile data on several common scanning devices that can be selectively invoked (e.g., by the user), depending on the particular scanner used.) The scanned image data is then processed by the application to infer the characteristics of the user's printer or software (e.g., its transfer function). Once these characteristics are known, the watermarking process can pre-compensate for such printer/software characteristics so as to produce a watermark whose attributes are largely independent of the printer/software from which it was generated. (E.g., if a printer exhibits attenuated reproduction of high frequency image data, the high frequency components can be pre-emphasized prior to sending the watermark data to the printer. Similarly, if the dot pitch produced by the printer emphasizes particular spatial frequencies, the watermark image data can be pre-compensated to de-emphasize such spatial frequencies.)

In other embodiments, the transfer functions of printing systems commonly used by users can be pre-characterized by the manufacturer, and appropriate compensation of watermark printing can be based thereon. Thus, for example, if a user is printing postage using a Hewlett-Packard LaserJet 8000DN printer, a first set of pre-stored pre-compensation information is utilized. If the user is printing using a Hewlett-Packard DeskJet 860C, a second set of pre-compensation information is utilized, etc. (The specification of the particular printer being used can be left to the user, or it can be determined by reference to data available in the computer system (e.g., by reference to the printer driver file being employed.))

The net result, again, is to make the printed end-product substantially uniform regardless of the idiosyncrasies of particular printing systems. (Further information on characterizing the transfer function

of devices to assure reliable watermark communication is found in copending application 60/173,880, filed December 30, 1999.)

In some embodiments, a hardware security device that is used, e.g., to store postage value (e.g., a digital vault) may also be employed by the watermark embedding system, e.g., as a source of secure and potentially unique data used in encoding the digital watermark (e.g., crypto keys, pseudo-random noise data, etc.). In some such arrangements, the watermark embedding system may make use of data stored in such device primarily for another purpose (e.g., a user ID), and can employ such data in conjunction with the watermarking operation (e.g., as a seed to a random number generator that produces a noise pattern utilized in the watermark encoding).

In accordance with still further embodiments of the invention, the principles described herein are also applicable to other printed value documents (e.g., tickets and coupons), especially those that are printed on demand. Such documents may be printed at home, at special kiosks (e.g., in-store), or by commercial printing establishments (i.e., mass produced). Among other functionality, the watermarks in such value documents can be used by investigators to distinguish originals from reproductions (by use of fragile watermarks), to authenticate documents (e.g., in ticket reading machines), and to link to associated internet resources. (An example of the latter is a ticket to a sporting or theatrical event that, when presented to a web cam, allows the user to see an actual or virtual view of the sports arena/stage from the perspective of the ticketed seat.)

The watermarks on printed value documents can also be linked to other information (e.g., event date, seat number, product code, etc.) that is textually printed on the document, or present on the document in some machine readable form (e.g., barcodes). In such case, the watermark can be used to detect document alteration by checking for discrepancy between the watermark-encoded information, and that otherwise conveyed by the document.

In accordance with still other embodiments, blank paper stock can be digitally watermarked so that printed documents formed by later printing on the stock exhibits desired functionality. (The watermark in the blank stock persists through, and is detectable notwithstanding, subsequent printing.)

For example, blank paper stock can be digitally watermarked with a frail watermark that permits the original document to be distinguished from photocopies or other reproductions. Or blank stock used as corporate stationary can be watermarked with data serving as an internet link to the corporation's web site. Or serialized sheets can be employed by a corporation for sensitive memoranda, allowing a printed document to be distinguished from seemingly-identical documents, e.g., permitting the document to be traced back to its original intended recipient

As in the examples earlier given, the watermark can be formed by ink (e.g., speckles, or tinting) or by texture. The watermark can be formed on the paper in bulk - in the paper-making process, or can be applied on a per-sheet basis. In the former case, the same watermark payload is encoded on large lots of paper, whereas in the second case, different watermark payloads can be applied to different sheets (e.g.,

serialized paper). (The later process can be performed by high-speed printing machines specialized for this purpose, e.g., employing page-width ink-jet arrays.)

(Watermarking of blank paper stock is referenced in various of the assignee's applications, including 09/127,502 and 09,619,264, as well as in patent 5,822,436.)

It will be recognized that the arrangements described above can be combined and hybridized in various ways to economically effect multiple functionality.

To provide a comprehensive disclosure without unduly lengthening this specification, the patents and applications cited herein are incorporated herein by reference.

Having described and illustrated the principles of the invention with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while digital watermarking typically does not leave any human-apparent evidence of alteration or data representation, certain of the foregoing applications do not require this. The markings used may be visible, and even conspicuous, without impairing essential functionality. Thus, bar codes, data glyphs, OCR markings, and other machine-readable indicia may be substituted, depending on the particular application requirements.

While the detailed embodiments were described with reference to desktop computers, it is recognized that such devices will increasingly be supplanted by other digital appliances, including general purpose personal digital assistants, multifunction cell phones, and specialized devices – many of which include integrated optical sensors (e.g., CCD or CMOS cameras). Moreover, the power and utility of the above-detailed embodiments and devices can be further enhanced by employing various wireless communications technologies, including the Bluetooth standard.

The implementation of the watermark encoding and decoding systems is straightforward to artisans in the field, and thus not belabored here. Conventionally, such technology is implemented by suitable software, stored in long term memory (e.g., disk, ROM, etc.), and transferred to temporary memory (e.g., RAM) for execution on an associated CPU. In other implementations, the functionality can be achieved by dedicated hardware, or by a combination of hardware and software. Reprogrammable logic, including FPGAs, can advantageously be employed in certain implementations.

While the specification makes reference to "paper" and "envelopes," these terms are used in shorthand fashion to refer to articles delivered by the postal service. Thus, postcards (e.g., direct mail cards) and Tyvek articles are meant to be encompassed by such references. Postcards may include multiple watermarks, e.g., a postal-related mark on the "address side," and an internet-linking mark on the other. The two marks may be associated or linked in various manners.

Although not described in the context of existing postal meters, it should be recognized that the above-detailed technology is well-suited for implementation with such devices, as they generally use printing techniques that are suitable for digital watermark printing. By retrofitting existing postal meters, a great variety of security and marketing improvements can readily be provided.

The reader will recognize that a variety of additional security techniques can be employed in conjunction with the arrangements detailed above. For example, in some applications, it is useful to encrypt the message encoded in the watermark. Encryption provides an additional layer of security to prevent unwanted uses of the encoded information. Some examples of applicable cryptographic methods include RSA, DES, IDEA (International Data Encryption Algorithm), skipjack, discrete log systems (e.g., El Gamal Cipher), elliptic curve systems, cellular automata, etc.

These and other cryptographic methods can be used to create a digital signature to place in a watermark message. Public key cryptographic methods employ a private and public key. The private key is kept secret, and the public key is distributed. To digitally sign a message, the originator of the message encrypts the message with his private key. The private key is uniquely associated with the originator. Those users having a public key verify that the message has originated from the holder of the private key by using the public key to decrypt the message.

The message may be both encrypted and digitally signed using two stages of encryption. At the encoder, a digital signature stage encrypts at least part of the message with a private key. An encryption stage then encrypts the message with a public key. The decoder reverses the process. First, a decryption stage decrypts the message with a private key corresponding to public key used in the encryption stage at the encoder. Then, a second stage decrypts the output of the previous stage with the public key corresponding to the private key used to create the digital signature.

Time and date stamping can be used in conjunction with encryption, or otherwise (e.g., in a watermark). Metadata can similarly be conveyed.

If desired, a watermark can be used to track mail (e.g., an envelope or parcel) through the delivery process. At various check points, a camera- or sensor-equipped device reads the watermark, extracts an identifier and logs the identifier along with additional information, such as location, time, etc. This information may be sent and maintained in a database that can be queried to determine the delivery status of the mail. Wireless devices can be employed to read watermarks and report status to a centralized or distributed database.

It should be recognized that the particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

WE CLAIM:

1. An original envelope having encoded thereon a fragile digital watermark representing plural bits of digital data, said watermark permitting a photocopy thereof to be distinguished from the original.

2. The envelope of claim 1 in which the watermark is formed with ink.

3. The envelope of claim 1 in which the watermark is formed by texturing of the original envelope medium

4. The envelope of claim 1 that additionally has encoded thereon a second digital watermark that withstands at least certain photocopying operations.

5. The envelope of claim 4 in which the second digital watermark encodes data useful for linking to an internet computer site.

6. The envelope of claim 4 in which the second digital watermark encodes data representing a device or user that produced the document.

7. The envelope of claim 4 in which one of said watermarks indicates to compliant equipment that the envelope should not be reproduced.

8. The envelope of claim 4 in which the second digital watermark is printed on the envelope at the same time as a franking mark.

9. The envelope of claim 8 in which the second digital watermark is printed on the envelope by the same printing assembly used to print said franking mark.

10. The envelope of claim 4 in which at least one of said digital watermarks occupies a region that is also occupied by a franking mark printed on said envelope.

11. The envelope of claim 4 in which the second watermark is formed on a second side of the envelope, opposite a side on which the first watermark is formed.

12. The envelope of claim 1 in which said digital watermark is printed on the envelope at the same time as a franking mark.

13. The envelope of claim 1 in which said digital watermark is printed on the envelope by the same printing assembly used to print said franking mark.

14. A blank original substrate suitable for later use in a printing operation to produce a printed document, the blank original substrate having encoded thereon a fragile digital watermark representing plural bits of digital data, said watermark permitting a photocopy thereof to be distinguished from the original.

15. The substrate of claim 14 in which the watermark is formed with ink.

16. The substrate of claim 14 in which the watermark is formed by texturing of the substrate medium.

17. A printed document comprising the substrate of claim 14 that additionally has encoded thereon a second digital watermark that withstands at least certain photocopying operations.

18. The document of claim 17 in which the second digital watermark encodes data useful for linking to an internet computer site.

19. The document of claim 17 in which the second digital watermark encodes data representing a device or user that produced the document.

20. The document of claim 17 in which the second watermark is formed on a second side of the envelope, opposite a side on which the first watermark is formed.

21. The substrate of claim 14 in which the watermark indicates to compliant equipment that the envelope should not be reproduced.

PRINTING MEDIA AND METHODS EMPLOYING DIGITAL WATERMARKS

Abstract of the Disclosure

Digital watermarks are encoded on envelopes to serve a variety of purposes related to postage (franking), anti-counterfeiting, addressing, and linking to associated internet sites. Digital watermarks can also be formed on blank paper stock so that printed documents formed therewith have desired properties, including the ability to distinguish photocopies from originals, to link to corporate web sites, and to permit document serialization for tracing and other purposes.

APPENDIX L

Watermarking a Carrier on Which an Image Will be Placed or Projected

Field of the Invention:

The present invention relates to Steganography and more particularly to digital watermarks.

Background of the invention:

There is a large body of art dealing with the technology for inserting digital watermarks into images and for reading such watermarks. In general the known techniques for inserting a digital watermark into an image involve changing some property of selected bits or pixels in an images. The pixels or bits are changed in a pattern that represents or carries certain data. The data carried by a digital watermark is often termed the "payload".

In general digital watermarking technologies seek to accomplish some or all of the following goals or objectives: First, the changes made in an image should not be visible to the normal observer. Second, the changes should be such that they can be detected and the payload can be read by a watermark reading program. Third, actions such as rotating, enlarging or manually handling an image should not prevent the watermark from being detected and read.

The important point relative to the present invention is that in the prior art watermarking technologies the watermark is applied to the image, text, audio, etc which will then carry the watermark. With the present invention, a pattern representing a watermark is deposited on a substrate or screen on which an image will be printed or projected.

Summary of the Present Invention:

With the present invention, a carrier is watermarked and then an image is printed or displayed on this carrier. A watermark can then be read from the image. If the image is printed on the carrier, the watermark can be read from the printed image or from any copy of the printed image. If the watermark is displayed on the carrier, and the displayed image is then copied, the copies will bear the watermark.

Brief Description of the Drawings:

Figure 1 is a block diagram of the steps involved in practicing a first embodiment of the invention.

Figure 2 is a very much enlarged side view of a carrier that has been watermarked according to the present invention.

Figure 3 is a diagram representing a second embodiment of the invention.

Figure 4 is a block diagram of the steps in a second embodiment of the present invention.

Detailed Description.

There are many ways of determining the particular pixels in an image that must be changed or "tweaked" so that the image will carry watermark data. There is a large body of literature and many patents directed to various techniques for determining the appropriate changes that should be make in an image in order to digitally watermark the image. Likewise there is a large body of literature and many patents directed to techniques for detecting and reading watermarks.

The present invention is not directed to a way of selecting particular pixels that are to be changed in order to watermark and image. Likewise the present invention is not directed to a technique for detecting and reading watermarks. With the present invention, selecting pixels which are to be changed to imbed a particular watermark in an image and reading a watermark from an image can be done using the technologies that are know in the art.

The present invention is directed to a new technique for physically changing pixels in an image in order to watermark the image. The particular pixels which one desires to change can be selected using any of the known watermarking techniques. With the present invention, a carrier such as paper is physically coated in such a way that when a non-watermarked image is printed on the paper, the image will be watermarked and a watermark can be read from the image using conventional techniques.

In an alternate embodiment selected area of a movie screen are coated (or otherwise altered) so that if a non-watermarked image is projected onto the screen and a picture is taken of the projected image, the resulting recorded image will carry a watermark.

Figure 1 is a block diagram showing the steps involved in the first embodiment of the present invention. First as indicated by block 101 a pattern of pixels is printed on the paper using transparent wax. The pattern that is printed is the pattern used by the known watermarking techniques to carry watermark data.

The printing can be done using a thermal wax printer such as the thermal wax printed manufactured by Tektronix, Inc. of Wilsonville, Oregon and marketed under the trademark "The Phaser 200. Alternatively the printing can be done using an ink jet printer. A wide variety of transparent thermal materials can be used. For example a transparent thermal wax of the type described in issued patent 6,018,082 can be used. The material which is used in this step of the process should be such that it does not create visible pattern to someone looking at the paper and it should have an effect on subsequently applied ink so that the

resulting image has a different characteristic in area where the material is located.

Next, as indicated by block 2, an image is printed using a conventional printer such as a conventional ink jet printer. There will be a slight difference between a pixel that is printed over a location where there is a wax layer and a pixel printed over a location where there is no wax pixel. The wax prevents, to some extent, the ink from being absorbed into the paper. The amount of wax (or other material) applied in the first step can be adjusted to insure that the differences between the areas where there is wax and the areas where there is not wax is such that the differences are not noticeable to a human observer, but the differences are sufficient that they can be detected by a watermark reading program.

Figure 2 illustrates (in greatly exaggerated fashion) the result of the steps indicated by blocks 101 and 102. As illustrated in Figure 2, the printing done in steps 101 and 102 is done on a substrate (e.g. a sheet of paper) 201. There are two layers on top of the substrate 201. Each layer is only present in certain selected pixel area. The first layer 202 consists of transparent wax printed at selected locations on the paper. The locations where the transparent wax is printed constitute the pattern of a digital watermark. On top of the transparent wax 202 is an ink image 203. Not illustrated in Figure 2 is the fact that in layer 203, the ink diffuses into the paper less in the areas where transparent wax 202 is located.

Block 103 is shown in dotted lines since it is an optional step. The image created in step 102 may or may not be copied using a conventional photocopier. As is well know, in general, when a watermarked image is photocopied, the resulting copy also containes the digital watermark.

Block 104 indicates that either the image printed in step 102 or the copy made in step 103 is scanned to create a digital image. Finally as indicated by block 105, a watermark is detected and read from the digital image using a conventional watermark reading program.

Figure 3 illustrates an alternative embodiment of the invention. The invention can be used to watermark images projected onto a movie screen so that if a recording is made from a movie screen the recorded images will bear a watermark.

This technology can be used to identify illegal copies made when a movie is shown in a legitimate theater. The watermark contained in the illegal copy could identify the theater were the copy was make.

In this alternative embodiment, the movie screen is coated (or built) with areas that have a different reflectivity or light absorption quantities. The areas on the screen with this different quality are in a pattern that represents a digital watermark. The differences between the areas with different qualities is

adjusted so that the differences would not be visible to human viewers, but the differences would be sufficient that they could be detected by a watermark reading program.

As shown in Figure 3, in this embodiment a projector 302 projects a movie onto a screen 301. Screen 301 is coated (or built) with areas of different reflectivity or light absorption characteristics. These area are in a pattern that represents a digital watermark. Any material which slightly changes the reflectivity of the screen such as a very thin layer of white adhesive material can be used in this step of the process. The type, and thickness of the material applied would be selected so that it is not visible to a human observer but such that it creates enough of a difference in the projected image that copies of the image would be watermarked.

The process is illustrated by the block diagram in Figure 4. As indicated by block 401, the screen is coated with a pattern that resents a watermark. Next as indicated by block 402 a movie is projected onto the screen. As indicated by block 403, the projected images are recorded. Finally as represent by block 404 a watermark is read from the recorded images.

It is noted that some movie screens have holes which facilitate transmission of sound from speakers placed behind the movie screen. In an alternate embodiment of the invention, these holes are positioned to coincide with the picture elements which must be changed in order to digitally watermark the image with a particular watermark. Thus, the location of the holes is placed such that images projected on the screen are digitally watermarked and if the images on the screen are photographed or otherwise recorded, the recorded image will be watermarked.

In still another embodiment of the invention, the surface of the screen is slightly altered in selected area by an abrasive or sanding process. This can be done by selectively lightly sandblasting selective areas of the screen so as to alter the characteristic of the screen in these area. The areas which are altered are the areas that represent a digital watermark.

It is noted that in all the embodiments involving projecting an imager on a screen, the projected image can be a single image or the projected image may be a series of images, that is, a movie.

While the invention has been shown and described with respect to preferred embodiments, it will be appreciated by those skilled in the art that various other changes in form and detail can be made without departing from the sprit and scope of the invention.

I claim

1) A method of watermarking an image comprising the steps of,
applying a first material on a substrate in a pattern that represents a digital watermark, said first material being transparent, printing an image on said substrate, said image having different characteristics in the areas where said first material is located.

2) The method recited in claim 1 wherein said first material comprises a transparent wax.

3) The method recited in claim 1 wherein said first material is applied by using a wax sublimation printing process.

4) The method recited in claim 1 wherein said image is printed using an ink jet printing process.

5) The method recited in claim 1 wherein said first material is applied by using a wax sublimation printing process and said image is printed using an ink jet printing process.

5) A method of watermarking an image comprising the steps of,
applying a first material on a screen in a pattern that represents a digital watermark, projecting an image on said screen, said screen reflecting said image with different characteristics in the areas where said first material is located, whereby recordings of said projected image bear said digital watermark.

7) The method recited in claim 5 wherein said screen is a movie theater.

8) The method recited in claim 5 wherein a series of images comprising a movie is projected on said screen.

9) A method of watermarking recorded images comprising the steps of projected an image on a screen which has areas with different reflective characteristics in a pattern that represents a digital watermark, recording images from said screen, whereby the recorded images bear said digital watermark.

10) A material suitable for printing comprising a substrate and a layer of material positioned on said substrate in a pattern that represents a digital watermark, said material being invisible to the human eye and affecting any ink deposited on said substrate, whereby any image printed on said substrate will bear a digital watermark.

11) The method recited in claim 10 wherein said material is transparent.

12) The method recited in claim 10 wherein said material is a transparent wax.

13) The method recited in claim 10 wherein said printing is done by an inkjet printing process.

14) the method recited in claim 9 wherein a series of images comprising a movie are projected on said screen.

Abstract

A carrier is watermarked and then an image is printed or displayed on this carrier. A watermark can then be read from the image. If the image is printed on the carrier, the watermark can be read from the printed image or from any copy of the printed image. If the watermark is displayed on the carrier, and the displayed image is then copied, the copies will bear the watermark